

REVEAL

FP7-610928



REVEALing hidden concepts in Social Media

Deliverable D1.2a

Legal / regulatory requirements analysis – Intermediary liability for third party content

Editor(s):	Pieter-Jan Ombelet, Aleksandra Kuczerawy, Prof. Peggy Valcke
Responsible Partner:	ICRI-CIR – KU Leuven
Status-Version:	Final - v1.0
Date:	15/05/2015
EC Distribution:	Internal deliverable

Project Number:	FP7-610928
Project Title:	REVEAL

Title of Deliverable:	Legal/regulatory requirements analysis
Date of Delivery to the EC:	15/05/2015

Workpackage responsible for the Deliverable:	WP1 - User Requirements and Regulatory Framework
Editor(s):	Pieter-Jan Ombelet, Aleksandra Kuczerawy, Prof. Peggy Valcke
Contributor(s):	
Reviewer(s):	SINTEF
Approved by:	All Partners

Abstract:	The aim of this deliverable is to provide an analysis of the legal framework for the REVEAL project. Deliverable 2.1a focuses on the topic of Internet intermediary liability. This is a crucial aspect of safeguarding legally compliant project results.
Keyword List:	Internet intermediary, liability, mere conduit, caching, hosting, search engines, notice-and-take-down, notice-and-action, applicable law, E-Commerce Directive

DOCUMENT DESCRIPTION

Document Revision History

Version	Date	Modifications Introduced	
		Modification Reason	Modified by
V0.2	17/03/2015	Creation of the Document Structure	ICRI-CIR – KU Leuven
V0.3	02/04/2015	First Draft of the Document	ICRI-CIR – KU Leuven
V0.4	20/04/2015	Second Draft of the Document	ICRI-CIR – KU Leuven
V0.5	23/04/2015	Third Draft of the Document	ICRI-CIR – KU Leuven
V0.6	08/05/2015	Final Draft of the Document	ICRI-CIR – KU Leuven
V0.7	12/05/2015	Revision by SINTEF	SINTEF
V1.0	13/05/2015	Final Version of the Document	ICRI-CIR – KU Leuven

CONTENTS

EXECUTIVE SUMMARY	7
1 INTRODUCTION	8
2 LIABILITY OF INTERMEDIARIES	10
2.1 EU REGIME ON LIABILITY OF INTERMEDIARIES – E-COMMERCE DIRECTIVE 2000/31/EC	11
2.1.1 Scope	12
2.2 LIABILITY EXEMPTIONS FOR INTERMEDIARIES.....	13
2.2.1 Mere Conduit	14
2.2.2 Caching	15
2.2.3 Hosting.....	17
2.2.4 No general obligation to monitor.....	19
2.3 LEGAL VACUUM OF SEARCH ENGINES IN THE EU	20
2.4 CRITICISM OF THE CURRENT FRAMEWORK	23
2.5 INTERMEDIARY LIABILITY ASPECTS IN THE EUROPEAN CASE LAW	24
2.5.1 Google Spain (CJEU)	25
2.5.2 Delfi (ECtHR).....	27
3 REVIEW OF THE E-COMMERCE DIRECTIVE.....	29
3.1 NOTICE AND ACTION INITIATIVE.....	29
3.2 LESSONS LEARNED	30
3.2.1 Legal uncertainty	30
3.2.2 Knowledge vs. complexity	30
3.2.3 Notifying content providers	31
4 APPLICATION TO REVEAL.....	33
4.1 ROLE OF REVEAL AS AN INTERMEDIARY	33
4.2 LEGAL RECOMMENDATIONS FOR REVEAL PLATFORM (HOW TO COMPLY WITH THE CURRENT REGIME).....	35
5 CONCLUSIONS.....	36
6 REFERENCES.....	37

LIST OF FIGURES

FIGURE 1: STYLISED REPRESENTATION OF INTERNET INTERMEDIARIES’ ROLES. SOURCE: OECD, THE ECONOMIC AND SOCIAL ROLE OF INTERNET INTERMEDIARIES 8

DEFINITIONS, ACRONYMS AND ABBREVIATIONS

Acronym	Title
ECD	E-Commerce Directive
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
CJEU	Court of Justice of the European Union
CDA	United States Communications Decency Act
DMCA	United States Digital Millennium Copyright Act
NTD	Notice and Take Down
N&A	Notice and Action
OECD	Organisation for Economic Co-operation and Development
SNS	Social Networking Sites
UGC	User Generated Content

Executive Summary

Deliverable 1.2a is the second legal deliverable of the REVEAL project. In the first year of the project legal research focused mainly on the privacy and data protection aspects in REVEAL to make sure that the project is conducted ethically and does not infringe fundamental human rights of individuals (see Deliverable D1.2).

Deliverable D1.2a extends the scope of the legal research within this project to an analysis of the Internet intermediary liability regime in the European Union. It provides legal and regulatory requirements that should be complied with during the project lifetime and later, during the exploitation phase. The ultimate objective of this deliverable is to guide the REVEAL partners towards compliance with European legislation in the area of Internet intermediaries.

REVEAL platform will facilitate access to content created by third parties (user generated content, UGC). If the content is illegal (e.g. defamatory or violating copyrights) REVEAL platform could potentially become liable as a contributor to the wrongdoing, because of REVEAL's involvement in disseminating the content. For that reason REVEAL partners must become familiar with the liability exemption regimes of the E-Commerce Directive. Considering the specificity of the REVEAL platform, the deliverable focuses primarily on the hosting exemption regime. The deliverable looks also into the situation of search engines in the EU legal framework.

Other legal aspects of the REVEAL project, namely compliance with the API Terms and Conditions of the underlying social networks and media law, will be addressed at the later stage of the project. Compliance with the API Terms and Conditions will be analysed from both legal and technical perspective. Together with practical recommendations it will form an annex to the presented deliverable. Media law aspects of the project will be discussed in year 3 of the project (D1.2b).

1 Introduction

So far the attention of the legal reports in this project was devoted mainly to the issues of privacy and data protection. Since REVEAL develops tools and services that aid in Social Media verification, the privacy of SNS users is a very sensitive issue that dominated the discussions in the first year of the project.

In the second year, attention needed to be given to other topics as well. The second legal deliverable of the REVEAL project addresses the questions related to the current legal situation of Internet intermediaries, since the REVEAL platform will serve as an Intermediary, storing and facilitating access to User Generated Content.

Internet intermediaries are actors, who are placed between two (or more) different parties to intermediate between them. They function as enablers of the communications between these parties. The Organisation for Economic Co-operation and Development (OECD) defines the role of Internet intermediaries as *'bring[ing] together or facilitat[ing] transactions between third parties on the Internet. They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties.'*¹

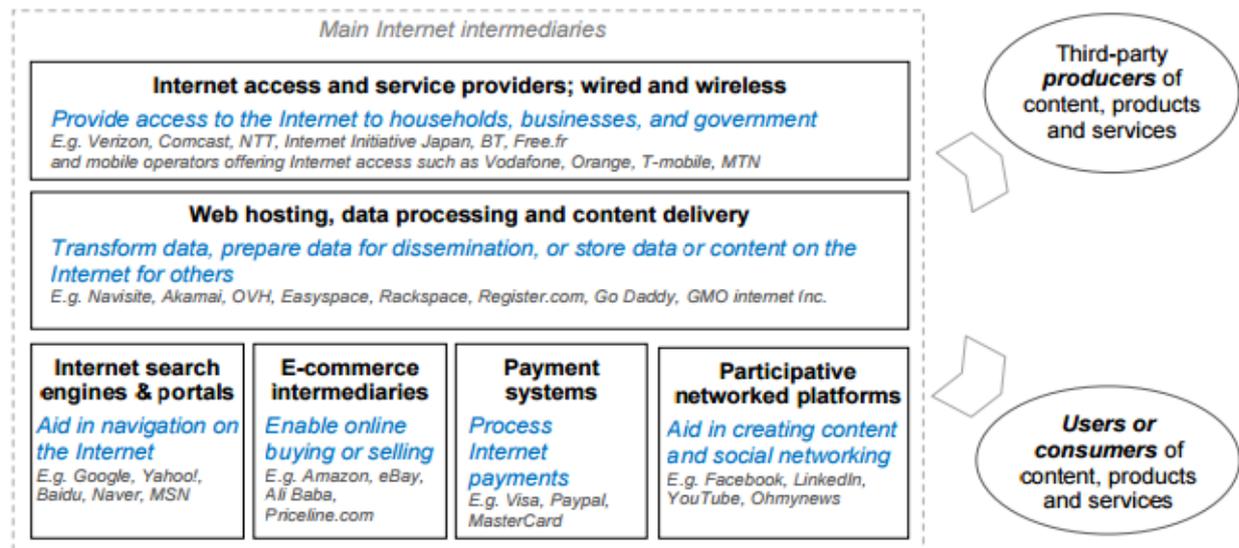


Figure 1: Stylised representation of Internet intermediaries' roles. Source: OECD, The Economic and Social Role of Internet Intermediaries

The deliverable provides a coherent overview of the legal framework governing the liability of the Internet intermediaries for the third party content in the European Union. More in detail, the present deliverable provides an analysis of the special regime for intermediaries provided in the E-Commerce Directive 2000/31/EC. Chapter 2 of this deliverable elaborates on the relevant sections of the Directive and define the conditions, with which different intermediaries need to be in compliance. The deliverable focuses on the EU legal framework because Member State legislation in this area stems from the EU law. The REVEAL project will, in the beginning, most likely, be deployed in

¹ OECD, The Economic and Social Role of Internet Intermediaries, April 2010, p. 9.

Greece. For this reason, the deliverable points out differences between the EU framework and Greek law where they arise. Later on in the exploitation phase it might be deployed in other EU Member States (e.g. in Germany). The conducted analysis of the EU regime is applicable to all the EU countries.

After outlining the key provisions of this directive, the deliverable provides two recent European case studies. Both *Google Spain* before the Court of Justice of the European Union and *Delfi* before the European Court of Human Rights are highly relevant in the context of REVEAL. *Google Spain* focuses on a type of Internet intermediaries (search engines) whose legal position is still quite unclear and largely undefined at the EU level. Furthermore, it constitutes a great case-study to assess the interaction between the intermediary liability regime and data protection law. The *Delfi* case on the other hand focuses more on the difference between Internet intermediaries (*in casu* platform providers) and professional publishers. It shines a new light on the liability of these providers for third party content on the platform.

The review process of the E-Commerce Directive led by the European Commission since 2010 is discussed in Chapter 3. More specifically, the chapter looks into the actions undertaken by the Commission on the topic of the Notice and Action initiative. Chapter 4 of the deliverable analyses the position of the future REVEAL platform from the perspective of the intermediary liability regime. It also provides recommendations for compliance with the E-Commerce Directive regime.

2 Liability of Intermediaries

New methods of communication and collaboration, citizen journalism and civic participation on the Internet has resulted in universal economic, political and social development. New technologies provided by Internet intermediaries, allow every individual to interact, share and express opinions with a wide and diverse audience. Citizens feel increasingly empowered by these easy and instant ways of communicating and expressing their opinions. Such empowerment is able to influence social and political interactions and shape current events. For example, intermediaries such as Social Networking Sites (SNS) enable individuals to keep up with an international network of friends as well as allow organizations to target audiences with specific interests. In the area of political interactions, one could mention the role the new methods of communication played in the Arab spring, the 'Occupy' movement and more recently the Ferguson unrest and Charlie Hebbo shooting. These methods are, however, also often perceived as a double-edged sword. Numerous copyright infringements, defamatory allegations and a myriad of illegal content being distributed online has made the ideal image of a free flow of information subject to vivid criticism. The absence of editorial control of User Generated Content (UGC) by certain intermediaries shows a strong opposition with traditional publishing and broadcasting. In traditional publishing or broadcasting certain deliberation is given to the selection of the material by the publishers or broadcasters due to their potential responsibility for the content. On blogs, discussion groups or SNS, no editorial control is used to select suitable content. Since there is no selection process, responsibility seems to be placed entirely on the author, who, if anonymous, might be impossible to discover. In such case, those harmed by the author's wrongdoing come knocking on the intermediaries' door in search of a remedy.

Examples of intermediaries, are internet service providers (ISPs), hosting providers, search engines, e-commerce intermediaries, Internet payment systems and participative Web platforms.² Their role is to 'provide access to, host, transmit and index content originated by third parties on the Internet; facilitate interactions or transactions between third parties on the Internet; or provide other Internet-based services to third parties'.³ Certain authors call intermediaries a natural point of control for content online, as they are actually enablers of Internet communications.⁴ As will become apparent in this deliverable, these entities differ from traditional publishers, as the role they play in providing access to content online is largely of a mere technical nature. Their position of rather passive conduits closely relates to the role of distributors, which are not required to exercise any form of content control.⁵ Nevertheless, Internet intermediaries are technically capable to stop a wrongdoing by eliminating access to objectionable material. Often, intermediaries are also able to facilitate identification of wrongdoers.⁶ With such power at their hands, intermediaries are great candidates to play the role of gatekeepers. Governments realised that quickly, so rather than introducing centralised oversight and enforcement, they decided to enlist intermediaries for the realisation of their public policy objectives - combating illegal online content. In order to ensure intermediaries' coopeartion, governments introduced conditional liability exemption for third party content.

Liability of the Internet intermediaries for third parties' content was increasingly seen as a problematic issue. With no uniform approach and varying classifications of responsibility, authorship,

² OECD, The Economic and Social Role of Internet Intermediaries, April 2010, pp. 9-14.

³ Ibid.

⁴ Zittrain J., A History of Online Gatekeeping, Harvard journal of Law and Technology, Vol. 19, No. 2, 2006, p.258; Mapping Digital Media: The Media and Liability for Content on the Internet, C. Wong, J.X. Dempsey, Open Society Foundation, Reference Series No.12, 2011, p.14

⁵ Zittrain J., *I.c.*, p. 258; CompuServe, 776 F. Supp.; Prodigy, 1995 WL 323710.

⁶ Zittrain J., *I.c.*, p. 254.

and types of content there was a strong inconsistency across legal systems.⁷ To tackle this issue, and to provide some level of legal certainty, first the USA and shortly after the European Union developed a limited liability regime for Internet intermediaries. Since, the Internet industry, which perceived liability for third parties' content as a growing risk, contributed strongly to the debate through advocacy. An immunity was introduced to stimulate growth and innovation of the newly born technologies and provide positive incentives for further development. The introduced solution was considered 'practical, uniform, acceptable to industry and also protective of consumers, citizens, and businesses'.⁸

Two basic principles are internationally accepted with regard to liability exemption for Internet intermediaries: a) lack of responsibility of intermediaries for third-party content distributed on the Internet and for transactions taking place on their platform as long as they do not modify that content nor are aware of its illegal character; and b) no general obligation for intermediaries to monitor content.

The US Communications Decency Act (CDA) 1996 was the first act that addressed the issue. Section 230(c)(1) provides immunity from liability for providers and users of an 'interactive computer service' who publish information provided by others by stating that '*no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider*'. This provision covers any kind of illegal content, such as libel, defamation, child pornography or privacy, except intellectual property infringements. The latter form of violations were addressed in the Digital Millennium Copyright Act (DMCA) 1998. Certain groups of Internet intermediaries, namely mere conduits, hosts (that store or cache content posted by others), and linking tools such as search engines, are included in the safe harbour scheme of this act, provided they implement a 'notice-and-take-down' procedure. This procedure aims to remove content upon complaint from copyright owners and provides a policy for terminating the accounts of 'repeat infringers' in certain circumstances.

In the European Union, the question of liability of Internet intermediaries was first addressed in the E-Commerce Directive of 2000.⁹

2.1 EU regime on liability of Intermediaries – E-Commerce Directive 2000/31/EC

Directive 2000/31/EC¹⁰, commonly referred to as the E-Commerce Directive (ECD), regulates the liability of Internet intermediaries in the European Union. Following a proposal by the European Commission in 1998, the E-Commerce Directive was signed by the European Parliament and the Council of the EU in June 2000. Member States had time until January 2002 to implement the Directive in their national legal order.

⁷ Kuczerawy A., Legal and ethical analysis, SocloS deliverable D3.5, August 2012, p. 5.

⁸ OECD, Directorate for Science, Technology and Industry, Committee for Information, Computer and Communication Policy, The Role of Internet Intermediaries In Advancing Public Policy Objectives, Forging partnerships for advancing public policy objectives for the Internet economy, Part II, 22.06.2011, p. 72.

⁹ Directive 2000/31/EC of the European Parliament and the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce), O.J. 17 July 2000, L 178/1-16.

¹⁰ Directive 2000/31/EC of the European Parliament and the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce), O.J. 17 July 2000, L 178/1-16.

The Directive aims to establish a clear and general framework to cover certain legal aspects of electronic commerce in the internal market.¹¹ As highlighted in the preamble of the Directive, the development of information society services within the Community is hampered by a number of legal obstacles to the proper functioning of the internal market which make less attractive the exercise of the freedom of establishment and the freedom to provide services. These obstacles further arise from divergences in legislation and from the legal uncertainty as to which national rules apply to such services.¹² The Directive addresses these issues in its two main objectives. In first instance, it sets out to remove certain legal obstacles which are seen as hindering the development of electronic commerce within the internal market. Simultaneously, the directive aims to provide legal certainty and safeguard consumer confidence towards electronic commerce.¹³ The development of electronic commerce within the information society will stimulate economic growth and investment in innovation by European companies, and can also enhance the competitiveness of European industry.¹⁴

The E-Commerce Directive regulates several aspects of information society services including freedom of services, the treatment of electronic contracts, and liability issues, among others. After elaborating upon the scope of this Directive, we will focus on the liability provisions which are most relevant for the deployment of REVEAL Services.

2.1.1 Scope

The E-Commerce Directive applies to “information society services”, which have been defined as ‘any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services’ (see art. 2, a ECD)¹⁵. The notion of “information society services” covers a wide range of services. Examples of the services falling under this broad definition can be found in Recital (18) to the Directive. They may include (in so far as they represent an economic activity): online contracting, services providing transmission of information via communication networks, services providing access to a communication network, hosting of information, as well as services that do not give rise to on-line contracting, e.g. those offering online information or commercial communications or those providing tools that allow for search, access and retrieval of data.¹⁶ Search engines are therefore covered by this definition.

The definition of information society services contains four key elements. A particular service can be qualified as an information society service if it is provided for:

- remuneration;
- at a distance;
- by electronic means;
- at the individual request of a recipient.

The element of remuneration does not necessarily refer to the specific way in which the service is financed, but rather to the existence of an economic activity or an activity for which an economic

¹¹ Recital (7) of Directive 2000/31/EC.

¹² Recital (5) of Directive 2000/31/EC.

¹³ Recital (7) of Directive 2000/31/EC.

¹⁴ Recital (2) of Directive 2000/31/EC.

¹⁵ This provision refers back the definition in Article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC.

¹⁶ For more examples, see Recital (18) of Directive 2000/31/EC.

consideration is given in return.¹⁷ Information society services are therefore not restricted to services, which are remunerated by their recipients as such.¹⁸

The element “at a distance” simply means that the parties are not simultaneously physically present in the same particular place.¹⁹

“By electronic means” comprises every service that is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and the storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means.²⁰ This means that the service should also be sent and received with the use of electronic equipment. This requirement excludes the traditional distance selling methods, like mail-ordering, from the scope of this definition.²¹

“At the individual request of a recipient of services” means that the service is provided through the transmission of data on individual request.²² Visiting a website is considered to be a service on demand, since the recipient ‘requests’ the website when typing the URL or following a link.²³

Examples of information society services may include (in so far as they represent an economic activity): on-line contracting, services consisting of the transmission of information via communication networks, services providing access to a communication network, hosting of information, services providing search tools, etc.²⁴

Article 1 ECD also excludes a number of services and legal issues from its scope, such as:

- questions covered by the Data Protection Directive (art. 1 (5), b);
- questions relating to agreements or practices governed by cartel law (art. 1 (5), c);
- the activities of notaries or equivalent professions to the extent that they involve a direct and specific connection with the exercise of public authority (art. 1 (5), d).

2.2 Liability Exemptions for Intermediaries

The E-Commerce Directive regulates the liability of intermediary service providers in its Section 4. This part of the Directive introduces liability exemptions for certain types of intermediary services. Intermediary service providers shall not be liable for actions that could be considered as ‘mere conduit’ (article 12), ‘caching’ (article 13) or ‘hosting’ (article 14). Once the provider of intermediary services is compliant with the conditions foreseen by each article, the particular service will benefit from the respective exemption.

¹⁷ Any type of economic activity present will suffice. For example the costs of the service could also be covered by advertisement. (Lodder A., ‘Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, in Lodder A. and Kasspersen (eds.), *eDirectives: Guide to European Union Law on E-commerce – Article by Article Comments*, Kluwer Law international, 2002, p. 71.)

¹⁸ Recital (18) of Directive 2000/31/EC.

¹⁹ See art. 1, 2 of the Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations (O.J. L 217/18-26).

²⁰ See art. 1, 2 of Directive 98/48/EC. It is not required that every aspect of the overall service that is being provided takes place by electronic means nor that the final service consists of an immaterial good. See e.g. European Court of Justice, Case C-108/09, *Ker-Optika Bt. v ÁNTSZ Dél-dunántúli Regionális Intézet*, 2 December 2010 (applying Directive 2000/31/EC to the sale of contact lenses via the internet).

²¹ Lodder, A., *l.c.*, p. 71.

²² Art. 1, 2 of Directive 98/48/EC.

²³ Lodder, A., *l.c.*, p. 71.

²⁴ See recital (18) ECD for more examples.

These liability provisions of the Directive represent the balancing exercise that took place between EU policy makers and the online industry. On the one hand there was a concern from the Internet industry that if intermediaries were to be held liable for third party content on similar grounds as ‘publishers’, it could keep service providers from entering the market (cf. *supra*).²⁵ On the other hand, EU policy makers pointed out that Internet intermediaries could play an important role in combating illegal content online and by doing so enhance public trust in the Internet as a safe space for economic activity.²⁶

As these exemptions have a horizontal nature, they cover various types of illegal content (infringements on copyright law, defamation law, protection of minors, unfair commercial practices, etc.) and different kinds of liability (criminal, civil, direct, indirect).²⁷

If the conditions for being exempt are not met, the intermediary is not per se subject to liability. The sole effect is that the intermediary no longer falls under the immunity provided by the Directive.²⁸ The liability question is determined, taking into account the conditions for imposing liability under the national law(s) applicable to the case (e.g. copyright law or defamation law).²⁹

2.2.1 Mere Conduit

Article 12³⁰ provides for the liability exemption for providers of ‘mere conduit’ services, which are described as:

- those services which consist of the transmission in a communication network of information provided by a recipient of the service (‘transmission services’); and
- those services which consist of the provision of access to a communication network (‘access services’).

According to article 12, the service provider is not liable for the information transmitted, on condition that the provider:

- (a) does not initiate the transmission (of data);
- (b) does not select the receiver of the transmission; and
- (c) does not select or modify the information contained in the transmission.³¹

²⁵ OECD, Directorate for Science, Technology and Industry, Committee for Information, Computer and Communication Policy, The Role of Internet Intermediaries In Advancing Public Policy Objectives, Forging partnerships for advancing public policy objectives for the Internet economy, Part II, 22.06.2011, p. 12; Walden I, in: Bullesbach A., Poulet Y., Prins C. (eds.), *Concise European IT Law*, Kluwer Law International Alphen aan den Rijn, 2005, p. 248.

²⁶ OECD, *ibid.*, p. 12.

²⁷ Schellekens, M.H.M., *Aansprakelijkheid van Internetaanbieders*, Legal Dissertation, Tilburg, 2001, p. 216 and Helberger N., et al., ‘Legal Aspects of User Created Content’ in IDATE, TNO, IViR, *User-Created Content: Supporting a Participative Information Society*, Study for the European Commission (DG INFSO), December 2008, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1499333, p. 40.

²⁸ Kuczerawy A. and Ausloos J., ‘Case Study: European Union & Google Spain’, NOC Report on Internet Intermediaries Liability, 2014, forthcoming, 24 p.

²⁹ Jakobsen, S.S., ‘Mobile Commerce and ISP Liability in the EU’, *International Journal of Law and Information Technology* 2010, vol. 19 no. 1, p. 38; Van Eecke P., Truyens M., Legal analysis of a Single Market for the Information Society, New rules for a new age? a study commissioned by the European Commission’s Information Society and Media Directorate-General, November 2009. Chapter 6: Liability of Online Intermediaries, p.10. Available at: http://ec.europa.eu/information_society/newsroom/cf/document.cfm?doc_id=842.

³⁰ Greece transposed this exemption in Article 11 of the Presidential Decree 131/2003 (Government Gazette (FEK) A 116/16-5-2003). The discussion under this heading is also applicable to scenarios falling under Greek jurisdiction. For more information see Iglezakis J., *Cyber Law*, National Monograph, Greece, p.240.

³¹ This requirement does not cover manipulations of a technical nature which take place in the course of the transmission as they do not alter the integrity of the information contained in the transmission (recital 43).

Recital (42) further stipulates that the exemptions from liability only cover cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network. The recital highlights that this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored.³² The services described in article 12 therefore can be compared to postal services, as the providers of these services are also not held liable for possible illegal content in the letters.³³

The acts of transmission and provision of access include the automatic, intermediate and transient storage of the information transmitted as long as this takes place for the sole purpose of carrying out the transmission in the communication network, and only if the information is not stored for any period longer than is reasonably necessary for the transmission (article 12.2).

Even if the intermediary is exempt from liability (i.e. when the conditions of article 12 are met), the possibility remains for a court or administrative authority to require the service provider to terminate or prevent an infringement, where the legal system of the Member State provides for this (article 12.3).³⁴

In practice only a limited group of service providers, such as telecommunications operators and ISPs, will benefit from the 'mere conduit' exemption.³⁵ Given the far-reaching restrictions associated with this exemption, it is expected that none of the actors involved in the provisioning of REVEAL Services will fall under the scope of this exemption under the Directive.

2.2.2 Caching

The second liability exemption provided by the Directive relates to 'caching' of information. Providers of 'proxy-servers'³⁶ are mainly targeted by this provision.³⁷ Article 13³⁸ defines caching as 'the automatic, intermediate and temporary storage of that information, performed for the sole purpose of

³² While recital (42) purports to address all of the exemptions of the Directive, one might argue that the scope of this part of the recital should be limited to the transmission and access services identified in articles 12 and 13. After all, the exemption for hosting identified in art. 14 does not limit its scope to either transmission or access services. See also Montéro, E., 'Les responsabilités liées au web 2.0', *Revue du Droit des Technologies de l'Information* 2008, n° 32, p. 367. However, the ECJ has held recital (42) equally applicable to hosting services: see European Court of Justice, Joined Cases C-236/08 to C-238/08, 23 March 2010 (Google France and Google v. Louis Vuitton Malletier a.o.), paragraphs 113-114.

³³ Lodder, A., *l.c.*, p. 87.

³⁴ See also CJEU, Case C 314/12, 27 March 2014 (UPC Telekabel Wien) on this matter. In this case, UPC Telekabel Wien, an internet service provider, received an injunction to block access of its users to a website making available to the public copyright infringing material (§2). The Court of Justice of the European Union found that the injunction was legitimate as long as the injunction does not specify the measures which that access provider must take and when that access provider can avoid incurring coercive penalties for breach of that injunction by showing that it has taken all reasonable measures. The measures taken also cannot unnecessarily deprive internet users of the possibility of lawfully accessing the information available. They further stated that the measures have to have the effect of preventing unauthorised access to the protected subject-matter or, at least, of making it difficult to achieve and of seriously discouraging internet users who are using the services from accessing the subject-matter that has been made available to them in breach of the intellectual property right (§63-64).

³⁵ Certain Member States have however broadened the scope of their national legal framework to cover services provided by other intermediaries such as for example search engines: Verbiest T. et al., *Study on the Liability of Internet Intermediaries*, commissioned by the European Commission, 12 November 2007, p.4, 19, available at: http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf.

³⁶ A proxy server is an intermediary server between the Internet user and the Net. It acts as a Web cache, dramatically improving the rate of display of information (e.g. the display of web pages). Article 29 Working Party, 'Working Document – Privacy on the Internet – an integrated EU Approach to On-line Data Protection', 21 November 2000, p. 10, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp37_en.pdf.

³⁷ Van Eecke P., Truyens M., 'Legal analysis of a Single Market for the Information Society, New rules for a new age? a study commissioned by the European Commission's Information Society and Media Directorate-General, November 2009. Chapter 6: Liability of Online Intermediaries', p.8.

making more efficient the information's onward transmission to other recipients of the service upon their request'. Service providers will only benefit from this exemption when the information society service they provide consists of the transmission in a communication network of information provided by a recipient of the service ('transmission services').

Recital (43) applies to caching of information, as well as 'mere conduit', since caching is equally limited to manipulations of a technical nature, which do not alter the integrity of the information contained in the transmissions.

Moreover, when comparing the 'mere conduit' exemption with the exemption for caching of information, the wording seems to be very similar. The recipient of the service in both cases provides the 'automatic, intermediate and temporary storage' of information. Still, the exemption for caching services only applies to transmission services (whereas the 'mere conduit' exemption prescribed in article 12. 2 formally extends to access services)³⁹.

The biggest difference between article 12.2 and 13.1 appears to relate to the purpose of the storage. When comparing the respective provisions, article 12.2 on mere conduit aims to exempt transient storage which takes place for the '*sole purpose of carrying out the transmission*'. Caching on the other hand is performed '*for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request*'.⁴⁰ Doctrine has agreed that this means that the storage under article 13.1 can be longer than the 'mere conduit' storage provided by article 12.2.⁴¹

The following five conditions must further be met in order to benefit from the caching exemption (article 13.1):

- *the (service) provider does not modify the information;*
- *the provider complies with conditions on access to the information;*
- *the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;*
- *the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and*
- *the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.*

³⁸ Greece transposed this exemption in Article 12 of the Presidential Decree 131/2003. The discussion under this heading is also applicable to scenarios falling under Greek jurisdiction. For more information see Iglezakis J., Cyber Law, National Monograph, Greece, p.241.

³⁹ The mere conduit exemption of art. 12, 2 also pertains to the activity of transmission rather than access provisioning. Nevertheless, due to the differences in structuring of the respective provisions, it would appear that strictly speaking only information society services which qualify as transmission services benefit from art. 12, 3, whereas both transmission services and access services are able to avail themselves of art. 12, 2.

⁴⁰ An example of the former would be the storage involved in "packet switching transmission" performed by ISP's; whereby information is stored for shorter period of time in small pieces (see Baistrocchi, P.A., 'Liability of intermediary service providers in the EU Directive on Electronic Commerce', *Computer & High Technology Law Journal* 2002, vol. 19, 119). An example of caching is the server or proxy caching performed by ISP's, whereby they conduct automatic, intermediate and temporary storage of popular websites in order to speed up the users access to the website (see Jakobsen, S.S., *l.c.*, 43).

⁴¹ Lodder A, *l.c.*, p. 88.

Just as for 'mere conduits', the caching exemption shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement (article 13.2).

Here too, none of the actors involved in the provisioning of REVEAL Services seem to qualify for the exemption under article 13.

2.2.3 Hosting

Article 14 of the Directive⁴², covering the third liability exemption for Internet intermediaries, provides that where an information society service consists of the storage of information provided by a recipient of the service, the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

- the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
- the provider, upon obtaining such knowledge or awareness, immediately removes or disables access to the information.

The typical service falling under this provision is a webhosting service that provides webspace to its users, where they can upload content to be published on a website (e.g. YouTube).⁴³

The storage by these 'hosting' service providers differs from 'mere conduit' and 'caching' transient storages in the sense of the purposes for which the storage takes place.⁴⁴ Hosting service providers do not store information merely 'incidental' when providing their transmission or access services, as is the case with 'mere conduit' and 'caching' services.⁴⁵ In the case of hosting services, this type of storage can be provided for a prolonged time period, and even be the primary object of the service.⁴⁶ The Court of Justice of the European Union (CJEU) has clarified that the exemption only applies to providers that conduct their services in a neutral sense. Neutral conduct has been defined by the Court as 'technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores.'⁴⁷

The EU countries have struggled with the difference of article 14.1a between 'actual knowledge' of the service provider for criminal liability and the less stringent 'constructive knowledge' for civil claims

⁴² Greece transposed this article in Article 13 of the Presidential Decree 131/2003. The discussion under this heading is also applicable to scenarios falling under Greek jurisdiction. For more information see Iglezakis J., *Cyber Law*, National Monograph, Greece, p.243-244.

⁴³ Van Eecke P., Truyens M., *Legal analysis of a Single Market for the Information Society, New rules for a new age? a study commissioned by the European Commission's Information Society and Media Directorate-General*, November 2009. Chapter 6: Liability of Online Intermediaries, p.9.

⁴⁴ Kuczerawy A. and Ausloos J., *l.c.*, p. 6.

⁴⁵ Walden I, in: Bullesbach A., Poulet Y., Prins C. (eds.), *l.c.*, p. 253.

⁴⁶ It has been said that this exemption was originally aimed at ISP's providing space on their internet servers for third parties' websites, or bulletin boards or chat room services provided by the ISP itself (where the ISP only provides technical means for the users' communication without interfering with the content being communicated between the users) (Jakobsen, S.S., *l.c.*, 44). However, the exemptions provided by the E-Commerce Directive are defined in functional terms (i.e. in terms of the activity being performed), not in terms of the qualification of the actor. While the European legislator arguably only envisioned providers whose services consisted mainly, if not exclusively, in the performance of operations of a strictly technical nature, the scope of the exemption may also be applied to other entities (provided the conditions set forth by art. 14 are met). As a result, the exemption may in principle benefit any type of service provider who stores content at the request of the recipient; including so-called 'web 2.0' service providers (see Montéro, E., *l.c.*, 369-373).

⁴⁷ Court of Justice of the European Union, Joined Cases C-236/08 to C-238/08, 23 March 2010 (Google France and Google v. Louis Vuitton Malletier a.o.), paragraphs 113-114. The European Court of Justice addressed the issue of neutrality of hosting service providers also in the L'Oréal eBay case. The Court ruled that art. 14 of the Directive applies to hosting providers if they don't play an active role that would allow them to have knowledge or control of the stored data. Court of Justice of the European Union, Case C-324/09, 12 July 2011 (L'Oréal v. eBay), paragraphs 112 - 116.

for damages.⁴⁸ The interpretations of ‘actual knowledge’ in the Member States range from knowledge obtained through a court order, to a sufficiently substantiated informal notice by a user.⁴⁹ On the other hand, ‘constructive knowledge’ is often understood as general awareness of the service provider.⁵⁰ The CJEU is aware of this divergence within the Member States.⁵¹ In *L’Oréal v. Ebay*, the Court stated that a service provider will only be exempt from any liability for unlawful data that it has stored on condition that it did not have ‘actual knowledge of illegal activity or information’.⁵² With regard to claims for damages, the service provider has to prove that it was not ‘aware of facts or circumstances from which the illegal activity or information is apparent’ or that, having obtained such knowledge or awareness, it has acted expeditiously to remove, or disable access to, the information.⁵³ The provider will be denied the exemption, when it should have been aware of facts or circumstances on the basis of which a diligent economic operator could have identified the illegality in question.⁵⁴ The threshold that the CJEU imposes in this case is quite high, since any diligent economic operator who is confronted with the material should identify it as being illegal.⁵⁵

Recital (46) further stipulates that ‘the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level’. These procedures for service providers are however not further regulated in the Directive, nor are there any other details or safeguards to ensure proportionality or due process of the removal or blocking.⁵⁶ Therefore, the assessment as to whether the notices of illegality are reliable enough to act upon has proven to be difficult for the providers.⁵⁷ Article 14.3 does prescribe the possibility for every Member State to establish ‘procedures governing the removal or disabling of access to information’. However, while some of the Member States have provided a more detailed regulation for the ‘hosting’ exemption by introducing formal notification procedures (‘Notice-and-Take Down procedures: cf. *infra*), many have left this possibility of the Directive unattended.⁵⁸

A hosting service provider further cannot benefit from the exemption of article 14 when the recipient of the service is acting under the authority or the control of the provider (article 14.2). For example if the service recipient service is an employee of the service provider, the latter will not qualify for the exemption if the content was introduced pursuant to its instructions.⁵⁹

Lastly, article 14 foresees the same possibility for a national court or administrative authority to introduce prohibitory injunctions as the articles on mere conduit and caching (article 14.3).

⁴⁸ See for example: BGH, 23/09/2003, VI ZR 335/02; Dutch Supreme Court 25 November 2005, LJN Number AU4019, case number C04/234HR; M. Turner (ed.) & J. Llevat, “The Spanish Supreme Court clarifies the concept of actual knowledge in connection with ISP’s liability”, *Comp LSR* 2010, volume 26, issue 4, 440-441 via Kuczerawy A. and Ausloos J., *l.c.*, p. 7-8.

⁴⁹ European Court of Justice (Grand Chamber), C-324/09, 12 July 2011, (*L’Oréal SA* and others).

⁵⁰ Kaspersen, H. and Lodder, A. (eds.), *E-directive: guide to European Union law on e-Commerce: commentary on the directives on distance selling, electronics signatures, electronic commerce, copyright in the information society, and data protection*, Den Haag, Kluwer, 2002, p. 88-89; Kuczerawy A., *Intermediary Liability & Freedom of expression: Recent developments in the EU Notice & Action Initiative*, *Computer Law and Security Review* 2015, vol. 31, Issue 1, p. 51.

⁵¹ European Court of Justice (Grand Chamber), C-324/09, 12 July 2011, (*L’Oréal SA* and others).

⁵² Paragraph 119.

⁵³ Paragraph 119.

⁵⁴ Paragraph 120.

⁵⁵ Van Eecke, P., *Online Service Providers and Liability: a Plea for a Balanced Approach*, *Common Market Law Review* 2011, vol. 48, issue 5, p. 1467.

⁵⁶ Kuczerawy A. and Ausloos J., *l.c.*, p. 8.

⁵⁷ Barceló R. J. and Koelman, K., ‘Intermediary Liability In The E-Commerce Directive: So Far So Good, But It’s Not Enough’, *Computer Law & Security Report* 2000, vol. 4, pp. 231-239, p. 231.

. The solution proposed by the Directive resembles the ‘notice and take down’ procedure of the US Digital Millennium Copyright Act. The American solution, however, introduces a set of formal requirements and a minimal content for the notices. Moreover, the DMCA includes also a ‘put back’ procedure, which gives an opportunity to recipients of the service to defend themselves in case the material is in fact legal. (Lodder, A., *l.c.*, p. 89.)

⁵⁸ First Report on the Application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on the Directive on Electronic Commerce, COM(2003) 702 final, Brussels, 21.11.2003.

⁵⁹ Lodder, A., *l.c.*, p. 89.

As will be explained in detail below, the solution applied to REVEAL will be based on the hosting regime.

2.2.4 No general obligation to monitor

Article 15 ECD⁶⁰ states that Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor to actively seek facts or circumstances indicating illegal activity.

The prohibition of monitoring obligations of article 15 refers solely to monitoring of a general nature. Member States are therefore only prevented from imposing a monitoring obligation on service providers with respect to obligations of a general nature; this does not concern monitoring obligations in a specific case nor does it affect orders by national authorities in accordance with national legislation (recital 47). Obliging service providers to conduct general monitoring of content would counteract the notice-and-take-down limited liability paradigm.⁶¹ They would no longer act passive and neutral. Moreover, general monitoring could even lead to censorship and have a consequential deterrent effect on the freedom of expression.⁶² The negative consequence of general monitoring is commonly referred to as a ‘chilling effect’.⁶³ The phenomenon occurs when individuals stop exercising a right or freedom, for example freedom of expression, out of a fear of potential repercussions.⁶⁴

This Directive further does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities (recital 48).⁶⁵ The duties of care are never defined in the Directive, which inadvertently blurs the difference between these duties and general monitoring. Recital 48 and article 15 can therefore be seen as quite contradictory.⁶⁶

Also, it is necessary to emphasise that the prohibition of general monitoring schemes according to article 15 only applies to service providers that provide ‘mere conduit’, ‘caching’ or ‘hosting’ services. If certain service providers fall outside the scope of these regimes, Member States theoretically could try to impose general monitoring obligations on them.⁶⁷ So far, there have been no such attempts in Europe.

⁶⁰ Greece transposed this provision in Article 14 (1) of the Presidential Decree 131/2003. The discussion under this heading is also applicable to scenarios falling under Greek jurisdiction. For more information see Iglezakis J., *Cyber Law*, National Monograph, Greece, p.242.

⁶¹ OECD, Directorate for Science, Technology and Industry, Committee for Information, Computer and Communication Policy, *The Role of Internet Intermediaries In Advancing Public Policy Objectives, Forging partnerships for advancing public policy objectives for the Internet economy*, Part II, 22.06.2011, p. 15, available on <http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP%282010%2911/FINAL&docLanguage=En>.

⁶² OECD, *I.c.*, p. 36.

⁶³ European Court of Human Rights, *Mosley v. United Kingdom*, nr. 48009/08, 15 September 2011.

⁶⁴ Van Alsenoy, B., Kuczerawy, A. and Ausloos, J., *Search engines after Google Spain: internet@liberty or privacy@peril?*, ICRI Working Paper Series, issue 15/2013, 6 September 2013, p. 48.

⁶⁵ The CJEU has in this regard decided, in two cases concerning the instalment of a filtering system to prevent the sharing of copyright infringing files, that an injunction obligating service providers to install a filtering system for all information which is passing via its services or stored on its servers by its users would constitute a general monitoring obligation if it applies indiscriminately to all of the users (1) as a preventative measure (2) exclusively at the provider's expense (3) and for an unlimited period (4), and if it is capable of identifying electronic files containing musical, cinematographic or audio-visual work of which the applicant holds intellectual property rights, with a view to preventing those works from being made available to the public in breach of copyright (Court of Justice of the European Union, C-70/10, 24 November 2011 (*Scarlet v. SABAM*), and Court of Justice of the European Union, C-360/10, 16 February 2012 (*SABAM v. Netlog*)).

⁶⁶ Barceló R. J. and Koelman K, *I.c.*, p. 232.

⁶⁷ See Jakobsen, S.S., *I.c.*, 43.

Lastly, article 15.2 gives Member States the possibility to impose two additional obligations upon information society services providers. First of all, they may oblige the providers promptly to inform the competent public authorities of alleged illegal activities by recipients. Secondly, the Member States may impose an obligation upon these providers to communicate to the competent authorities, at their request, the identity of recipients with whom they have storage agreements.

2.3 Legal vacuum of search engines in the EU

Considering the functionalities - such as search, identification, location and discovery functionality - that REVEAL plans to deploy, we need to address one more type of intermediary – search engine services.

Search engines are a type of selection intermediary, also called information location services or referencing services. Their role is to map, order, select, validate and value online information.⁶⁸ In doing so, they help users to navigate the Web and provide them with a way to overcome its information overload.⁶⁹ Search engines therefore ensure the free flow of information and deliver a crucial service in today's society. It could be argued that by providing access to information and diverse opinions, they participate in guaranteeing freedom of expression, as prescribed by article 10 of the European Convention of Human Rights (ECHR).^{70,71} It is therefore critical to examine the liability of the providers of this type of services for the third party content to which they link or provide access to.

Search engines are covered by the definition of the Information Society Service from the E-Commerce Directive. In Recital 18 it is stated that: '[I]nformation society services are not solely restricted to services giving rise to on-line contracting but also, in so far as they represent an economic activity, extend to services which are not remunerated by those who receive them, such as those offering on-line information or commercial communications, or those providing tools allowing for search, access and retrieval of data...'

Location tool services, however, are not covered by any of the three definitions of the services described in Section 4 of the E-Commerce Directive. They are, strictly speaking, neither a mere-conduit service, nor caching or hosting service. This implies that the liability exemptions for intermediaries of article 12-15 ECD do not cover, at least nominally, search engines and hyperlinks. The Directive, therefore, leaves this issue unattended.⁷² Only in the Final Provisions of the Directive, the problem is mentioned on the list of topics that should be analysed in future, during the re-examination of the document. More specifically Article 21 the Directive states that: 'in examining the need for an adaptation of this Directive, the report shall in particular analyse the need for proposals concerning the liability of providers of hyperlinks and location tool services...'⁷³

⁶⁸ Van Hoboken J., Legal Space for Innovative Ordering: on the need to update selection intermediary liability in the EU, *International Journal of Communications Law & Policy*, Issue 13, Winter 2009, pp.49-69.

⁶⁹ Van Hoboken J., *ibid*; Nathenson I. S., *Internet Infoglut and Invisible Ink: Spamdexing Search Engines with Meta Tags*, 12 *HARV. J.L. & TECH.* 43 (1998); Pasquale F., *Copyright in an Era of Information Overload: Toward the Privileging of Categorizers*, 60 *VAND. L. REV.* 133 (2007).

⁷⁰ Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms*, CETS No. 005, 04.11.1950, Rome, retrieved from <http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm>.

⁷¹ Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines, (Adopted by the Committee of Ministers on 4 April 2012 at the 1139th meeting of the Ministers' Deputies).

⁷² EU Study on the Legal analysis of a Single Market for the Information Society, *New rules for a new age? Part 6. Liability of online intermediaries*, November 2009.

⁷³ Directive 2000/31/EC, art. 21(2).

This means that, until now, the legal situation of search engines with regard to liability for third party content is not regulated in the E-Commerce Directive. It is not clear from the legislative history why the European Commission has so far ignored the topic. The preparatory stages only allow us to assume that search engines were still a developing technology, not popular enough to be included in the drafting works.⁷⁴

Since the E-Commerce Directive reserved itself from regulating this issue, it was left entirely to the discretion of the Member States. Some of the countries have used this possibility, according to the EC's first report on the application of the E-Commerce Directive.⁷⁵ The result is an amalgam of diverse approaches to this issue across the EU.

Some countries extended the scope of the legislation transposing the E-Commerce Directive to include search engines. Among those Member States two approaches can be distinguished. In some countries, like for example Austria, these types of services were classified as providers of access services (mere-conduit). The reasoning behind this choice was that 'search engines generally do not edit the content they show in the results, are not the source of the information they link to, and are not in the position to remove it from the Web'.⁷⁶ Other Member States, such as Spain⁷⁷, Portugal⁷⁸ and Hungary⁷⁹, opted for the hosting regime of art. 14 ECD to cover search engine providers. As stated above, this exempts providers of these services from liability if they do not have knowledge of the illegal nature of the information. They must further act expeditiously when they obtain such knowledge.

The third group of the EU countries so far has left this issue unregulated and apply the general rules of law. The example here is the U.K. which is waiting for the European Commission to introduce legislation on this issue.⁸⁰ A similar situation can be found in Germany and the Netherlands, where the general rules of law, particularly tort law, are applied.⁸¹ Very often, this lack of specific legislation

⁷⁴ Van Hoboken J., Legal Space for Innovative Ordering: on the need to update selection intermediary liability in the EU, *International Journal of Communications Law & Policy*, Issue 13, Winter 2009.

⁷⁵ First Report on the Application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, at 13, COM (03) 0702, (November 21, 2003), available at: http://www.instinformatica.pt/servicos/informacao-e-documentacao/biblioteca-digital/areas-aplicacionais/erpscom/com2003_0702en01.pdf/at_download/file (last visited Jan. 27, 2009).

⁷⁶ See footnote 30 in: Van Hoboken J., Legal Space for Innovative Ordering: on the need to update selection intermediary liability in the EU, *International Journal of Communications Law & Policy*, Issue 13, Winter 2009.

⁷⁷ See art. 17 of Law 34/2002 on Information Society Services and Electronic Commerce (Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico) of Jul. 12, 2002 (B.O.E. 2002, 166) (Spain). For a short overview of the Spanish implementation of the Directive on Electronic Commerce, see Rosa Julia- Barceló, Spanish Implementation of the E-Commerce Directive. Main features of the Implementation of the Ecommerce directive in Spain, 2002 *COMPUTER UND RECHT INTERNATIONAL* 112.

⁷⁸ See Decreto- Lei n.º 7/2004, de 7 de Janeiro, que transpõe para a ordem jurídica nacional a Directiva n.º 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de Junho, relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio electrónico, no mercado interno; Decreto-Lei 62/2009; Official Journal: Diaro da Republica I, number: 48, Publication date: 10/03/2009, p. 01602-01602 (MNE(2009)51108) <http://www.cnpd.pt/bin/legis/nacional/DL62-2009-SPAM.pdf>.

⁷⁹ See 2001. évi CVIII Törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről [Act CVIII of 2001 on Electronic Commercial Services and Certain Legal Aspects of Information Society Services] (promulgated 24 Dec., 2001), *MAGYAR KÖZLÖNY [HUNGARIAN GAZETTE]* 2001/153, translated in <http://www.nhh.hu/dokumentum.php?cid=11961>.

⁸⁰ DTI Consultation Document on the Electronic Commerce Directive: The Liability of Hyperlinkers, Location Tool Services and Content Aggregators - Government Response and Summary of Responses 6 (December 2006), available at <http://www.berr.gov.uk/files/file35905.pdf>.

⁸¹ See Sieber U., Liesching M., Die Verantwortlichkeit der Suchmaschinenbetreiber nach dem Telemediengesetz [The Liability of Search Engine Operators after the Telemedia Act], *MULTIMEDIA UND RECHT [MMR]*, Issue 8/2007; Peter Ruess, 'Just Google it?' – Neuigkeiten und Gedanken zur Haftung der Suchmaschinenanbieter für Markenverletzungen in Deutschland und den USA ['Just Google it?' – Novelties and Thoughts on the Liability of Search Engine Operators for Trademark Infringement in Germany and the USA], 2007 *GEWERBLICHER RECHTSSCHUTZ UND URHEBERRECHT* 198 in: Van Hoboken J., Legal Space for Innovative Ordering: on the need to update selection intermediary liability in the EU, *International Journal of Communications Law & Policy*, Issue 13, Winter 2009.

leads to complex rulings of the respective national courts on the issue.⁸² Greece, where REVEAL will be most likely deployed, joins this third group of countries. The Greek Presidential Decree No. 131/2003 implementing the E-Commerce Directive 2000/31/EC, that came into effect on January 17th, 2002⁸³, does not address the issue of liability exemptions for the providers of location tool services such as search engines. This means that the liability of search engines for linking to infringing content is regulated by the general rules of law.⁸⁴

As can be seen from the short analysis above, liability of search engines for the third party content is far from harmonised at the EU level. The complexity of the issue and the varying national traditions create a situation of legal uncertainty that may be challenging for the providers of these services. This challenge is highlighted by the variety of decisions of numerous European courts with regard to the legal situation of Google⁸⁵ (cf. *infra*). However, this situation also poses considerable issues for emerging, smaller market players who, in most circumstances, cannot afford the elaborate legal services that are at Google's disposal. Legal fragmentation in the EU may constitute an obstacle to enter the field and as a result hamper innovation and competition in the European market.⁸⁶ Major multinational selection intermediaries therefore often prefer complying with the US law, as it provides them with the liability exemptions required to ensure their lawful operation.⁸⁷

To eliminate legal uncertainty and safeguard the free flow of information on the Internet and the freedom of expression it is crucial to address the situation of search engines at the level of the European Community.

Such discussion has been put forth, to a very limited extent, at the beginning of the review of the Directive. In the published first report on the application of the Directive the Commission did not address the issue on intermediary liability and declared that: 'It is encouraging that recent case-law in the Member States recognises the importance of linking and search engines to the functioning of the Internet. In general, this case-law appears to be in line with the Internal Market objective to ensure the provision of basic intermediary services, which promotes the development of the Internet and e-commerce. Consequently, this case-law does not appear to give rise to any Internal Market concerns.'⁸⁸

The report was released in 2003, when several EU countries had not implemented the Directive yet. The situation has certainly changed since then, which is reflected by the recent initiatives of the European Commission with regard to the E-Commerce Directive.

⁸² Bundesgerichtshof [BGH][Federal Court of Justice] Jul 17, 2003, I ZR 259/00; Oberlandesgericht [OLG] Hamburg [Court of Appeals Hamburg], February 20, 2007, AZ. 7 U 126/06; Landesgericht [LG] Berlin [Trial Court Berlin], February 22, 2005, AZ 27 O 45/05.

⁸³ Presidential Decree No. 131/2003 (Government Gazette (FEK) A 116/16-5-2003) "Implementation of Directive 2000/31 of the European Parliament and of the Council on certain aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce)

⁸⁴ Iglezakis J., *Cyber Law*, National Monograph, Greece, p.230

⁸⁵ E.g. European Court of Justice, Joined Cases C-236/08 to C-238/08, 23 March 2010 (Google France and Google v. Louis Vuitton Malletier a.o.); Court of Appeal, Case no. 08/13423, 26 January 2011 (Société des Auteurs des Arts visuels et de l'Image fixe (SAIF) v Google France/Google inc.); The Court of Appeal of Brussels, Case no. 2007/AR/1730, 5 May 2011 (Copiepresse v. Google); Court of Milan, Case no. 1972/2010, 24 February 2010.

⁸⁶ Van Hoboken J., *Legal Space for Innovative Ordering: on the need to update selection intermediary liability in the EU*, *International Journal of Communications Law & Policy*, Issue 13, Winter 2009.

⁸⁷ Grimmelmann J., *The Structure of Search Engine Law*, 93 IOWA L. REV. 1 (2007); U. Gasser, *Regulating Search Engines: Taking Stock and Looking Ahead*, 8 YALE J. L. & TECH. 124 (2006).

⁸⁸ First Report on the Application of Directive 2000/31/EC, *supra* note 56.

2.4 Criticism of the current framework⁸⁹

The intermediary liability regime of the E-Commerce Directive has been criticised almost since the day it was introduced. Especially the fallacies of the hosting regime were analysed extensively.

One of the most problematic issues that stakeholders generally agree upon, is the lack of clarity of the current hosting regime. Burdening intermediaries with a task of assessing the legitimacy of a complaint and the character of the content has frequently been called unfair.⁹⁰ There are several reasons for such an opinion. Firstly, private companies often do not possess enough legal knowledge to evaluate the (il)legality of third party content. This is especially the case whenever the content is not manifestly illegal, which may occur where the subjective rights of individuals are at stake.⁹¹ Moreover, often undesirable effects can arise when enlisting private companies to decide upon such delicate issues.⁹² An example can be found in recent events during which Google was pressured to remove an offensive anti-Muslim movie from its YouTube platform.⁹³ In 2012, Google refused to comply with a request of the US government to remove the video, stating that no policies were infringed upon.⁹⁴ On the other hand Google arbitrarily decided to block access to the video from particular countries. It was consequently accused of paternalism and moral policing of the freedom of expression.⁹⁵

The specificity of the ‘notice-and-take down’ mechanism implies that intermediaries shall, as a rule, experience a conflict of interests. In essence, they have to remove or block content swiftly in order to exonerate themselves from possible liability. This essentially makes them a judge in their own cause. Therefore, they will have a natural tendency to choose the most cautionary approach and act upon any indication of illegality, without engaging in any (possibly burdensome and lengthy) balancing of fundamental rights that require protection. As a result, any analysis of the unlawful character of the content is usually non-existent.⁹⁶ In essence, the notice-and-take down mechanism will create ‘an incentive to systematically take down material, without hearing from the party whose material is removed, thus preventing such a party from its right to evidence its lawful use of the material’.⁹⁷ Aside from the obvious private censorship concerns⁹⁸, it also opens a way for fictitious victims such as competitors or political opponents to potentially abuse the mechanism.⁹⁹

⁸⁹ This part is based on Kuczerawy A., Intermediary Liability & Freedom of expression: Recent developments in the EU Notice & Action Initiative, *Computer Law and Security Review* 2015, vol. 31, Issue 1, 48-49

⁹⁰ Lievens E., Protecting Children in the Digital Era e the Use of Alternative Regulatory Instruments. Martinus Nijhoff Publishers, International Studies in Human Rights, Leiden, 2010, p. 360 (with reference Montero E., ‘La responsabilite des prestataires intermediaries sur les reseaux’, in: Montero E. (ed.), *Le commerce electronique europeen sur les rails?*, Cahiers du CRID, Brussel, Bruylant, 2001, 289e290).

⁹¹ Barcel_o R. J. and Koelman, K., *I.c.*; Barcel_o R. J., On-line intermediary liability issues: comparing EU and US legal frameworks, Electronic Commerce Legal Issues Platform, Deliverable 2.1.4bis, 16 December 1999, p. 13e17, available at: <http://www.glinks.net/lab991216/liability.doc>; The Organization for Security and Co-Operation in Europe and Reporters Sans Frontiers, Joint declaration on guaranteeing media freedom on the Internet, 17e18.06.2005, available at: <http://www.osce.org/fom/15657>.

⁹² Council of Europe (Council of Ministers), Declaration on freedom of communications on the Internet, 28.05.2003, p. 11, available at: <https://wcd.coe.int/ViewDoc.jsp?id=37031>.

⁹³ White House asked YouTube to review anti-Muslim film, David Nakamura, The Washington Post, 14.09.2012, at: <http://www.washingtonpost.com/blogs/post-politics/wp/2012/09/14/white-house-asked-youtube-to-review-anti-muslim-film>.

⁹⁴ Why Google Shouldn't Have Censored The Anti-Islamic Video, Eva Galperin, Techcrunch, 17.09.2012, at: <http://techcrunch.com/2012/09/17/why-google-shouldnt-have-censored-the-anti-islamic-video/>.

⁹⁵ YouTube under new pressure over anti-Muslim film, BBC News, 19.09.2012, available at: <http://www.bbc.com/news/technology-19648808>.

⁹⁶ Discussion in C. Ahlert, C. Marsden and C. Yung, “How Liberty Disappeared from Cyberspace: the Mystery Shopper Tests Internet Content Self-Regulation” (“Mystery Shopper”) at <http://pcmlp.socleg.ox.ac.uk/sites/pcmlp.socleg.ox.ac.uk/files/liberty.pdf>.

⁹⁷ Barcel_o R. J. and Koelman, K., *Op. Cit.* 20, p. 231.

⁹⁸ Barcel_o R. J., *Op. Cit.* 20, p. 13 e 17; Lievens E., *Op. Cit.* 19, p. 360.

⁹⁹ T. Verbiest et al., Study on the liability of Internet Intermediaries, Markt/2006/09/E, 12.11.2007, p.15, available at: http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf; OECD, The Economic and Social

A process whereby a private party, and possibly future defendant, decides arbitrarily whether content should be removed or blocked can lead to a violation of the right to freedom of expression, as enshrined in article 10 ECHR¹⁰⁰ and article 11 of the Charter of Fundamental Rights of the European Union.¹⁰¹ Concerns about a possible ‘chilling effect’ on the freedom of expression were voiced by a number of organisations, such as the Council of Europe.¹⁰² The notice-and-take-down mechanism moreover appears to be vying with the principles of proportionality and due process.¹⁰³

At the EU level, no guidelines were put forth concerning the implementation of notice-and-take down. The introduction of the actual procedures was left entirely to the discretion of the Member States. Recital 46 ECD explicitly confirms this discretion, by stating that the removal or disabling of access should be undertaken in observance of this right and of procedures established for this purpose at national level. In its article 16 and recital 40 the Directive encourages self-regulation in this field. Since the majority of the Member States chose for a verbatim transposition of the Directive, the matter was mostly left to self-regulation.¹⁰⁴ However, since most Member States never introduced any such measures, this self-regulatory system proved to be insufficient. The result is a lack of any firm safeguards in many jurisdictions.¹⁰⁵

2.5 Intermediary Liability aspects in the European case law

Before moving on to the review of the E-Commerce Directive, we should discuss two recent court judgments of the CJEU and the European Court of Human Rights (ECtHR). As a preliminary matter, it is worth highlighting the particular role of the European Convention of Human Rights (ECHR) within the EU legal order.¹⁰⁶ The ECHR was enacted by the Council of Europe, which is not an institution of the EU. In theory, the legal orders of these two international organizations are entirely distinct from each other.¹⁰⁷ However, all Member States of the European Union are also signatories, and therefore bound, to the ECHR.¹⁰⁸ In addition, the CJEU has explicitly recognized that EU Courts have to take the case law of the ECtHR into account when interpreting fundamental rights.¹⁰⁹ This means that the case law developed by the ECtHR and the CJEU are equally relevant to our current analysis.

Role of Internet Intermediaries, April 2010, ft. 83, available at: <http://www.oecd.org/internet/ieconomy/44949023.pdf>; Urban J. and L. Quilter, “Efficient Processes or Chilling Effects? Takedown Notices under Section 512 of the Digital Millennium Copyright Act,” 22 Santa Clara Computer & High Tech. L.J., 2006, p. 612.

¹⁰⁰ Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, CETS No. 005, 04.11.1950, Rome, available at: <http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm>.

¹⁰¹ Charter of Fundamental Rights of the European Union, 2000/C364/1, 18.12.2000, available at: http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

¹⁰² Council of Europe (Council of Ministers), Op. Cit. 21, p. 6; Council of Europe, Human rights guidelines for Internet Service Providers e Developed by the Council of Europe in co-operation with the European Internet Service Providers Association (Euro-ISPA), July 2008, paras 16, 21 and 24, available at: [http://www.coe.int/t/dgh/standardsetting/media/Doc/H-Inf\(2008\)009_en.pdf](http://www.coe.int/t/dgh/standardsetting/media/Doc/H-Inf(2008)009_en.pdf); C. Wong, J.X. Dempsey, Op. Cit. 1, p.16; See also: Electronic Frontier Foundation, “Takedown Hall of Shame,” available at <http://www EFF.org/takedowns>; and Chilling Effects Clearinghouse, available at <https://chnm.gmu.edu/digitalhistory/links/cached/chapter7/link7.62.ChillingEffects.html>.

¹⁰³ Horten M., The Copyright Enforcement Enigma e Internet Politics and the ‘Telecoms Package’, Palgrave Macmillan, 22 Nov 2011, p. 48-50.

¹⁰⁴ Verbiest T. et al., Op. Cit. 28, p. 14-16.

¹⁰⁵ Commission Staff Working Paper, Op. Cit. 7, p. 43-47.

¹⁰⁶ Van Alsenoy, B., Kuczerawy, A. and Ausloos, J., *I.c.*, p. 48.

¹⁰⁷ The dedicated enforcement mechanism of the ECHR is the European Court of Human Rights, whereas the final arbiter of the EU Charter is the European Court of Justice. The observance of the respect for fundamental rights within the EU is thus ensured by both the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR).

¹⁰⁸ The EU itself is not (yet) a party to the ECHR. This means that the ECHR and its judicial mechanism do not formally apply to EU acts. This divergence shall be rectified when the EU, as an organisation, will become a party to the Convention. The accession is currently negotiated. For more information see http://www.coe.int/t/dgh/standardsetting/hrpolicy/Accession/default_en.asp.

¹⁰⁹ See J. Kokott and C. Sobotta, ‘The Charter of Fundamental Rights of the European Union after Lisbon’, *European University Institute, Academy of European Law*, 2010/6, p. 2, available at <http://cadmus.eui.eu/handle/1814/15208>.

2.5.1 Google Spain (CJEU)

In 2009, a Spanish citizen found references to insolvency proceedings against him in a local newspaper (*La Vanguardia*) when he entered his name into Google's search engine. He was disturbed by this search result, as he already successfully settled all his debts in 1998 after a public auction referenced in the article. He asked the newspaper to remove the information in question, but this request was denied. He therefore requested Google's Spanish subsidiary to remove the article from the search results when somebody entered his name as a search term.¹¹⁰ They referred the complaint to Google Inc., as they considered them the responsible entity for the development of search results.

In March of 2010, L. asked the Spanish Data Protection Authority (*Agencia Española de Protección de Datos*, AEPD) to issue an administrative decision which would (a) order *La Vanguardia* to eliminate or modify the publication to ensure his personal data would no longer appear in search results; and (b) order Google to stop referring to the contentious publication in its search results.¹¹¹ In July 2010, the AEPD ordered Google Es. and Google Inc. to take 'all reasonable steps to remove the disputed personal data from its index and preclude further access.'¹¹² The request against *La Vanguardia* was denied, as – according to the AEPD – the newspaper still had a legitimate reason to process the data at issue.¹¹³ In 2011, Google appealed the AEPD's decision before the Spanish National Court (*Audiencia Nacional*) in Madrid.¹¹⁴ In March of the next year, this court referred the case to the CJEU for a preliminary ruling.¹¹⁵

The CJEU decided in their ruling of 13 May 2014 to counter the Advocate General's opinion of June 2013. Search engine operators fall within the scope of the European Data Protection framework. With regard to the so-called 'Right to be Forgotten', the court decided that data subjects can request search engines to remove a reference to a webpage when their name is used as a search term.¹¹⁶ The Court based this right to removal on the already existing right to erasure as enshrined in article 12 of the Data Protection Directive 95/46.¹¹⁷ It specified that the right to erasure is not absolute and a balance of rights and interests needs to be made.¹¹⁸ The interests at issue are the economic interests of the search engine and the legitimate interests of Internet users while accessing content on the one hand, and the data subject's rights on the other hand.¹¹⁹ The court indirectly confirmed that the burden of proof to establish which interests should prevail is on the search engine.¹²⁰

In this respect, the CJEU introduces a system that closely resembles the notice-and-take-down mechanism for hosting service providers (art. 14 ECD).

¹¹⁰ Audiencia Nacional. Sala de lo Contencioso, *Google Spain SL y Google Inc., S.L. c. Agencia de Protección de Datos*, paragraph 1.2, available at

<http://www.poderjudicial.es/search/doAction?action=contentpdf&database=AN&reference=6292979&links=%22725/2010%22&optimize=20120305&publicinterface=true>, paragraph 1.3.

¹¹¹ *Ibid*, paragraph 2.1

¹¹² *Ibid*, paragraph 2.3.

¹¹³ i.e. order issued by the Spanish Ministry of Labour and Social Affairs *Ibid*, paragraph 6.2.

¹¹⁴ Kuczerawy A. and Ausloos J., *I.c.*, 18.

¹¹⁵ At the risk of generalising too much, the request for a preliminary ruling contained two categories of questions: (a) the scope of application of European data protection law; and (b) the existence of a right to be forgotten/erasure vis-à-vis search engines directly.

¹¹⁶ Kuczerawy A. and Ausloos J., *I.c.*, 18-19. Such a right would be based on the rights to object (14) and to erasure (12(b)) in the Data Protection Directive.

¹¹⁷ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive), *O.J.* 23 November 1995, L 281

¹¹⁸ Paragraphs 74 *et seq.*

¹¹⁹ Kuczerawy A. and Ausloos J., *I.c.*, 19.

¹²⁰ Paragraph 81; 97.

The case nevertheless entirely hinges upon the European Data Protection legislation, which focuses on the activities of the controller, i.e. the search engine. A reference to the liability exemptions of the E-Commerce Directive is completely lacking. This can be explained by the different paradigms of data protection and intermediary liability law. Whereas the latter correlates strongly to traditional tort law principles (fault, damage and causal relationship) and the liability for illegal online content, data protection law simply provides certain responsibilities for controllers of personal data.¹²¹ No harm has to be proven under the data protection framework.¹²²

More interesting in the context of the REVEAL project is that the underlying content Google refers to often is published lawfully. Therefore, the publisher will not have a legal obligation to take it down.¹²³ This is different than within the notice-and-take-down mechanism, since the exemption regime of the E-Commerce Directive solely focuses on the illegal nature of the content.

With regard to the freedom of expression, Advocate-General Jääskinen emphasised the importance of this fundamental right in his opinion. He strongly believed that requesting search engine service providers to suppress legitimate and legal information that has entered the public domain *'would entail an interference with the freedom of expression of the publisher of the web page.'*¹²⁴

In the court judgment however, one notices instantly that there is less emphasis on the fundamental right to freedom of expression. The Court only confirms that a fair balance needs to be struck between the interests of internet users to access information and the data subject's rights. The Court stated that *'[w]hilst it is true that the data subject's rights protected by those articles [article 7 and 8 of the Charter] also override, as a general rule, that interest of internet users, that balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.'* By touching upon the right of access to information, the Court addressed the freedom of expression. The Court further touched upon the freedom of expression in their assessment of Article 7 (f) of the Data Protection Directive 95/46.¹²⁵ This article dictates a balancing exercise between the legitimate interests of the controller to process personal data and third parties to have this data disclosed on the one hand and the data subject's rights on the other hand. Here as well, the Court states that the application of this article necessitates a balancing of the opposing rights and interests concerned.¹²⁶ These paragraphs emphasise the importance of the freedom of expression. Not every breach of the data subject's rights will suffice to justify restriction on the freedom of expression and access to information (e.g. when information concerns a politician acting in the public sphere).

The Article 29 Working Party has further clarified that the right to erasure (or as we can call it after the ruling – the right to be delisted) only affects the results obtained from searches made on the basis of a person's name and does not require deletion of the link from the indexes of the search engine altogether. Therefore, the original information will remain accessible using other, often more

¹²¹ Kuczerawy A. and Ausloos J., *I.c.*, 20-21.

¹²² Article 23 of the Directive does provide for the possibility to obtain damages whenever someone is in fact harmed.

¹²³ In the Google Spain case, *La Vanguardia*, the original source, even had an explicit obligation to publish the information.

¹²⁴ Opinion of Advocate General Jääskinen, *Case C-131/12 Google Spain SL and Google Inc. vs. Agencia Española de Protección de Datos and Mario Costeja González*, 25 June 2013, paragraph 134.

¹²⁵ This provision permits the processing of personal data where it is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject — in particular his right to privacy with respect to the processing of personal data (Paragraph 74).

¹²⁶ Paragraph 74.

relevant, search terms or by direct access to the source.¹²⁷ The concerns with regard to the freedom of expression therefore seem to be undeniable, but should not be overstated.¹²⁸

2.5.2 Delfi (ECtHR)

The second case that concerns Internet intermediary liability in defamation actions is *Delfi v. Estonia*¹²⁹ case before the ECtHR. The *Delfi* case concerned an online news article from 2006 regarding a change in ferry routes delaying the opening of an ice road. This article was followed by 185 comments in the portal's 'Add Your Comment' section in 48 hours. Twenty of these comments were considered abusive and defamatory, as they involved personal threats and offensive language against a member (L.) of the ferry company's supervisory board.¹³⁰ In March 2006 L.'s lawyers requested the applicant company to remove the offensive comments and claimed for damages.¹³¹ Delfi thereafter removed the 20 messages in question promptly. Nevertheless, they refused to pay damages. Three weeks later, L. brought a civil suit against the applicant company.¹³²

Despite the local court ruling in favour of Delfi in first instance, both the Court of Appeal and the Supreme Court in Estonia overturned this decision. The Court of Appeal stated that Delfi could not rely on the national implementation of the E-Commerce Directive, i.e. the Estonian Information Society Services Act.¹³³ Moreover, the Court of Appeal decided that Delfi could not benefit from the notice-and-take-down regime of the ECD, as they were not merely a technical, automatic and passive intermediary. Instead, it invited users to add comments. Thus, the applicant company was a provider of content services rather than of technical services.¹³⁴

The Supreme Court later upheld the Court of Appeal's judgment in substance, partly modifying its reasoning.¹³⁵ The Court highlighted that just because the applicant company did not write the comments itself did not imply that it had no control over the comment environment. It enacted the rules of comment and removed comments if the rules were breached.¹³⁶ The fact that Delfi made no use of its possibility to prevent clearly unlawful comments from being published, was considered by the Court as an unlawful failure to act.¹³⁷

Delfi consequently appealed to the ECtHR, complaining that holding it liable for the comments posted by the portal's readers infringed its freedom of expression as provided by article 10 ECHR. The ECtHR confirmed the decision of the national appeal courts, and emphasised that *'the applicant company, by publishing the article in question, could have realised that it might cause negative reactions against the shipping company and its managers and that, considering the general reputation of comments on the Delfi news portal, there was a higher-than-average risk that the negative comments could go beyond the boundaries of acceptable criticism and reach the level of*

¹²⁷ Article 29 Data Protection Working Party, Guidelines on the implementation of the Google Spain judgment, available at http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20141126_wp29_press_release_ecj_de-listing.pdf.

¹²⁸ Nevertheless, it deserves to be highlighted that in this case the rights holder (i.e. the data subject) did notify Google Es. Therefore, from the perspective of the hosting exemption of the E-Commerce Directive, Google would have had to remove the content upon notification, even without the court judgment (Kuczerawy A. and Ausloos J., *I.c.*, 20)

¹²⁹ European Court of Human Rights, *Delfi AS. v. Estonia*, nr. 64569/09, 10 October 2013.

¹³⁰ Paragraph 13.

¹³¹ Paragraph 15.

¹³² Paragraph 17.

¹³³ Cheung, A.S.Y., 'Liability of Internet host providers in defamation actions: From gatekeepers to identifiers', in Koltay, A.

(Ed.), *Media Freedom and Regulation in the New Media World* (289-307), Budapest, Hungary: Wolters Kluwer, 2014, p. 292.

¹³⁴ European Court of Human Rights, *Delfi AS. v. Estonia*, nr. 64569/09, 10 October 2013, paragraph 25.

¹³⁵ Paragraph 26.

¹³⁶ Paragraph 27.

¹³⁷ Paragraph 29.

gratuitous insult or hate speech. Therefore, they defined Delfi as a professional publisher and not an Internet service provider, exempting them from the intermediary liability regime of the ECD.

Since the ruling by the national courts, Delfi has changed their policy and no longer allows persons who have posted offensive comments to post any new comments without reading and accepting the rules of commenting.¹³⁸

The confirmation by the ECtHR of the judgments of the domestic courts has been heavily criticised for creating a threat to freedom of expression. The Court's ruling encourages private censorship by Internet service providers and publishers of online news media.¹³⁹ The NGO Article 19 concluded that the Delfi judgment displayed 'a profound failure to understand the EU legal framework regulating intermediary liability'.¹⁴⁰ The NGO felt that Delfi had every reason to believe that the situation fell within the ECD's scope of protection since the company removed the material on the same day that it had received the complaint.¹⁴¹

Following this heavy debate, 69 media organisations, internet companies, human rights groups and academic institutions across Europe sent a joint letter in January 2014 to the ECtHR's president to support Delfi's appeal to the Court's Grand Chamber.¹⁴² In the letter, they emphasised the importance of maintaining no general obligation to monitor for intermediaries. The rule is considered a crucial guarantee for freedom of expression as it prevents overbroad monitoring and filtering of user content and, as a result, minimizes private censorship.

The Delfi judgment was eventually referred to the Grand Chamber of the ECtHR in February 2014. There has not yet been an end judgment. Further developments in this case will be closely monitored by Reveal.

¹³⁸ Cheung, A.S.Y., *I.c.*, 296.

¹³⁹ Voorhoof D., 'Recente rechtspraak belaaft expressievrijheid op internet', *De Juristenkrant*, 20 November 2013, 3; Voorhoof D., 'ISP of online uitgever. Delfi naar de Grote Kamer?', *Mediaforum* 2014/1, 1.

¹⁴⁰ Article 19, European Court strikes serious blow to free speech online, 14 October 2013, <http://www.article19.org/resources.php/resource/37287/en/european-court-strikes-serious-blow-to-free-speech-online>.

¹⁴¹ Article 19, *I.c.*

¹⁴² Re: Grand Chamber referral in Delfi v. Estonia (Application no. 64569/09), 13 January 2014, <https://www.laquadrature.net/en/civil-society-calls-on-the-echrs-grand-chamber-to-overturn-delfi-v-estonia-ruling>. This letter was also signed by the KU Leuven Interdisciplinary Centre for Law and ICT.

3 Review of the E-Commerce Directive

In 2010, the European Commission only started the process of reviewing the E-Commerce Directive by launching a public consultation as part of its periodic review process.¹⁴³ The main aim of this consultation was to establish whether a revision of the Directive was required. Stakeholders were generous in their responses, which were bundled by the European Commission in a report. The report documented the most often expressed complaints in general, and more specifically with regard to liability of intermediaries.¹⁴⁴ Most respondents agreed that there was no need for a revision of the ECD. Many stakeholders however emphasised that certain aspects of the directive would benefit from further clarification, particularly with regard to intermediaries' liability for third-party content. A more in depth analysis of the identified issues was further conducted by the European Commission in their Staff Working Document on Online Services.¹⁴⁵

3.1 Notice and Action Initiative

The most debated issue during the review process turned out to regard the functioning of the notice-and-take-down procedures. In the current Directive, the 'Notice and Take Down' (NTD) mechanism is implied in article 14 ECD (cf. *supra*). The 'Notice and Take Down' system hosting service providers benefit from the liability exemption if they 'act expeditiously' to remove or disable access to information upon obtaining knowledge or awareness of its illegal nature. In January 2012, following concerns revealed during the public consultation of 2010 about the lack of adequate safeguards to protect the freedom of expression, the European Commission announced a new initiative on 'Notice and Action'¹⁴⁶ (N&A) procedures.¹⁴⁷ The goal of this initiative is to set up a horizontal European framework for notice and action procedures, to combat illegal or infringing content on the Internet and to safeguard the transparency, effectiveness, and proportionality of Notice and Action procedures, as well as compliance with fundamental rights.¹⁴⁸ In June 2012, the European Commission launched a second public consultation, dedicated entirely to Notice and Action procedures applicable to hosting service providers. The following section will discuss three of the main problems with the intermediary liability regime (notice and take down), according to the public consultations and the Staff Working Document.¹⁴⁹

¹⁴³ See European Commission, "Online Services, Including e-commerce in Single Market", Commission Staff Working Paper, SEC(2011) 1641 final, p. 5, available at http://ec.europa.eu/internal_market/e-commerce/docs/communication2012/SEC2011_1641_en.pdf.

¹⁴⁴ Summary of the results of the Public Consultation on the future of electronic commerce in the Internal Market and the implementation of the Directive on electronic commerce (2000/31/EC), available at: http://ec.europa.eu/internal_market/consultations/docs/2010/e-commerce/summary_report_en.pdf.

¹⁴⁵ Commission Staff Working Document Online services, including e-commerce, in the Single Market, Brussels, 11.1.2012 SEC(2011) 1641 final.

¹⁴⁶ The main difference with Notice-and-Take Down is that in Notice-and-Action a broader range of actions against the content can be taken, providing a possibility for a tailored response (e.g. 'notice-and-notice' or 'notice-and-stay down'); *The notice and action procedures are those followed by the intermediary Internet providers for the purpose of combating illegal content upon receipt of notification. The intermediary may, for example, take down illegal content, block it, or request that it be voluntarily taken down by the persons who posted it online*. Commission Communication to the European Parliament, The Council, The Economic and Social Committee and The Committee of Regions, A coherent framework for building trust in the Digital Single Market for e-commerce and online services {SEC(2011) 1640 final}, p. 13, ft. 49, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0942:FIN:EN:PDF>.

¹⁴⁷ European Commission, "Commission Communication to the European Parliament, The Council, The Economic and Social Committee and The Committee of Regions, A coherent framework for building trust in the Digital Single Market for e-commerce and online services", SEC(2011) 1640 final, p. 13, ft. 49, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0942:FIN:EN:PDF>.

¹⁴⁸ Commission Communication, *l.c.*, p.14.

¹⁴⁹ For a more comprehensive discussion of these documents see Kuczerawy A., Intermediary Liability & Freedom of expression: Recent developments in the EU Notice & Action Initiative, *Computer Law and Security Review* 2015, vol. 31, Issue 1, 46-56.

3.2 Lessons learned

3.2.1 Legal uncertainty

Firstly, legal uncertainty is the most common criticism with regard to the N&A regime and more in general the E-Commerce Directive. The unclear scope of the definitions of intermediaries (cf. *supra*) were highlighted by the stakeholders in the public consultations and the Staff Working Document.¹⁵⁰ Very often, it is unclear for providers of ‘new’ types of services (e.g. video-sharing sites, SNS or search engines) to determine whether or not they could benefit from a liability exemption. Furthermore, this uncertainty pushes the intermediaries to be overly cautious. Wrongful notices, both in good and bad faith, present perhaps the greatest risk to freedom of expression in the current legal framework.¹⁵¹ Further, the stakeholders complained about the unclear conditions for exoneration.¹⁵² Terms such as ‘expeditiously’ and ‘actual knowledge’ were found to lead to different interpretations in various countries, and among the stakeholders.¹⁵³ Van Eecke for example argues that service providers do not have to perform a solely ‘passive role’ as long as they do not have ‘actual knowledge’ of the illegal nature of certain content.¹⁵⁴ And while this ‘storage but no knowledge’ approach seems fair¹⁵⁵, this in the end cannot alleviate all legal uncertainty.¹⁵⁶ Therefore, not only providers of online cross-border services but also users experience the functioning of the internal EU market in this regard as being quite problematic.¹⁵⁷

3.2.2 Knowledge vs. complexity

As stated above, article 14 ECD prescribes that hosting providers are exempt from liability in cases where the latter do not have actual knowledge of illegal activity or information. With regard to claims for damages, hosting service providers are exempt as long as they are not aware of facts or circumstances from which the illegal activity or information is apparent. This requirement of absence of knowledge requires intermediaries to conduct a legal assessment of the content. The assessment might be particularly difficult when the content is not manifestly illegal, for example when the conflicting interests involve subjective rights of individuals.¹⁵⁸ What is considered as ‘defamatory’ in one Member State is not necessarily categorised as such in another jurisdiction. The intermediaries will therefore often prefer to err on the side of caution and remove content, when not sure about their illegal nature. This leads to the elimination of disputed content, even if it is in fact legitimate.¹⁵⁹ Such approach could, however, be highly detrimental for freedom of expression. Similarly detrimental is the tendency of intermediaries to ‘race to the bottom’, in the sense that they will adopt the interpretation followed by the Member States with the most restrictive approach on content. Although regrettable for the freedom of expression, this choice is understandable as the intermediaries will hereby ensure less liability claims, and further keep their response consistent across different jurisdictions. The stakeholders, nevertheless, agreed that there should be a difference in treatment

¹⁵⁰ Commission Staff Working Document, *I.c.*, p. 32-39.

¹⁵¹ Kuczerawy A., *I.c.*, 52.

¹⁵² Kuczerawy A., Intermediary Liability & Freedom of expression: Recent developments in the EU Notice & Action Initiative, *Computer Law and Security Review* 2015, vol. 31, Issue 1, 50.

¹⁵³ Commission Staff Working Document, *I.c.*, p. 32-39.

¹⁵⁴ Van Eecke P., “Online Service Providers and Liability: a Plea for a Balanced Approach”, *Common Market Law Review*, Issue 5, p. 1463, 1472

¹⁵⁵ Van Eecke P., “Online Service Providers and Liability: a Plea for a Balanced Approach”, *I.c.*, p. 1472.

¹⁵⁶ Van Alsenoy B., Verdoodt V., Kuczerawy A. and Acar G., *I.c.*, p. 19.

¹⁵⁷ Kuczerawy A. and Ausloos J., “Case Study: European Union & Google Spain”, NOC Report on Internet Intermediaries Liability, 2014, forthcoming, 24 p.

¹⁵⁸ Barceló R. J. and Koelman K., *I.c.*, 231-239; The Organization for Security and Co-Operation in Europe and Reporters Sans Frontiers, Joint declaration on guaranteeing media freedom on the Internet, 17-18 June 2005, available at: <http://www.osce.org/fom/15657>.

¹⁵⁹ Kuczerawy A., Intermediary Liability & Freedom of expression: Recent developments in the EU Notice & Action Initiative, *Computer Law and Security Review* 2015, vol. 31, Issue 1, 50; Van Alsenoy B., Verdoodt V., Kuczerawy A. and Acar G., Evaluation of the legal framework applicable to Online Social Networks, Spion Deliverable D9.6.3, January 2015, p. 17.

between breaches of criminal and civil law: for example copyright infringements should receive a different assessment than child pornography. A one-size-fits-all approach might lead to either criminal or civil matters being handled in a disproportionate matter.¹⁶⁰

In this regard, the CJEU decided in *L'Oréal v. Ebay* that the liability exemption of article 14 would not apply once the service provider is 'aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality'.¹⁶¹ Therefore, the hosting service provider can only be held liable if it is sufficiently clear that the content at issue infringes upon the rights of others.¹⁶²

3.2.3 Notifying content providers

Notifying the content providers whose information will be removed proved to be another hot topic in the public consultations. Most civil society organisations argued that prior notification or consultation of the content providers was crucial. For example EDRI came to the conclusion that the US approach 'delete first, ask questions later' was contrary to the ECHR and Charter and should at all costs be avoided.¹⁶³ Other stakeholders emphasised that this prior notification should only be the case if content is not manifestly illegal.¹⁶⁴ For example, Bits of Freedom argued that 'if information is unmistakably unlawful and there is need to immediately disable access, the hosting provider can disable access right away'.¹⁶⁵ In such circumstances hosting providers should inform the content provider post-factum, and provide him with information regarding his rights of redress (in court). Business federations, on the other hand, sometimes disagreed that hosting service providers should consult the providers of alleged illegal content.¹⁶⁶ Alternatively, they felt that consultation with the providers of the content should occur after an action against the content has been taken. If it appears that the content was actually legal, it should be re-uploaded.¹⁶⁷

In its Staff Working Document, the European Commission considers the use of "counter-notices" to help protect freedom of expression.¹⁶⁸ Counter-notices can be found in the U.S. Digital Millennium Copyright Act (DMCA), which contains liability exemptions similar to those of the E-Commerce Directive.¹⁶⁹ Several EU Member States have also introduced an equivalent measure in their national NTD procedures, but it has not become a standard part of the procedure across Europe.¹⁷⁰ The objective of counter-notice mechanisms is to give the providers of allegedly illegal information a right to reply to the allegations of illegality of their content. Proponents argue that such a right to respond would introduce an important element of the due process. It would allow content providers to defend

¹⁶⁰ Netzpolitik response to the Consultation on Clean and Open Internet, https://netzpolitik.org/wp-upload/N_a_T_answers_digiges.pdf.

¹⁶¹ Court of Justice of the European Union, *L'Oréal v. eBay*, case C-324/09, paragraph 120.

¹⁶² Van Alsenoy B., Verdoodt V., Kuczerawy A. and Acar G., Evaluation of the legal framework applicable to Online Social Networks, Spion Deliverable D9.6.3, January 2015, p. 20.

¹⁶³ EDRI response to the Consultation on Clean and Open Internet, http://edri.org/files/057862048281124912Submission_EDRI_NoticeAction.pdf, p. 4.

¹⁶⁴ CDT response to the Consultation on Clean and Open Internet, <https://www.cdt.org/files/pdfs/CDT-Comments-Notice-and-Action.pdf>, p.7.

¹⁶⁵ Bits of Freedom (BoF), Response to the Consultation on Clean and Open Internet, <https://www.bof.nl/live/wp-content/uploads/040912-submissiontoformofconsultationeuropeancommission.pdf>, p.4.

¹⁶⁶ The European Telecommunications Network Operators' Association (ETNO), Response to the Consultation on Clean and Open Internet, available at <https://www.etno.eu/datas/positions-papers/2012/etnoc01-dsm-notice-and-action-consultation-sep-2012.pdf>, p.14

¹⁶⁷ European Communities Trademark Association (ECTA), Response to the Consultation on Clean and Open Internet, available at http://www.ecta.org/IMG/pdf/_ec.europa.eu_yourvoice_ipm_forms_dispatch.pdf, p. 4.

¹⁶⁸ *Ibid.*, p. 45.

¹⁶⁹ This similarity refers to the main concept of the NTD mechanism. The DMCA version of the mechanism contains a number of safeguards, which are absent in the e-Commerce version of NTD.

¹⁷⁰ In particular Finland, Hungary, Lithuania, Spain and UK. See more in: First Report on the Application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on the Directive on Electronic Commerce, COM(2003) 702 final, Brussels, 21.11.2003.

their use of the content, which in turn would result in a better assessment by the hosting provider.¹⁷¹ However, critics argue that a counter-notice mechanism would make the whole process more burdensome, slow and ineffective, and that it would not be appropriate in case of manifestly illegal content (e.g. child pornography). Most of this criticism originates, unsurprisingly, from the copyright industry. This group of stakeholders systematically emphasised the importance of efficiency of the take down process. From the perspective of the freedom of expression and due process, however, it seems that the legitimacy of Notice and Action would benefit from this counter-notice.

The Notice and Action initiative lost its momentum before the 2014 EU elections. Only recently, the European Commission brought back the intention to further work on combating the illegal content on the Internet. In the newest Digital Single Market strategy the Commission announces a comprehensive analysis of the role of platforms in the market including illegal content on the Internet, to take place in the course of 2015.¹⁷² We will have to see if the ideas of the Notice and Action initiative are continued or whether the Commission will be starting the process from scratch.

¹⁷¹ GNI, Comments on the Public Consultation on Procedures for Notifying and Acting on Illegal Content Hosted by Online Intermediaries, 5 September 2012, <http://globalnetworkinitiative.org/sites/default/files/GNI%20Comments%20on%20EC%20Notice%20and%20Action%20consult.pdf> However, some research indicates that, at least in the context of the DMCA, such counter-notice is rarely used in practice. This is because such counter-notification is considered an added cost, which individuals are not willing to take when exercising their right to speech. See more in: Seltzer W., The Politics of Internet Control and Delegated Censorship for The American Society of International Law, April 10, 2008; Seltzer W., Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment, Harvard Journal of Law & Technology, Volume 24, Number 1 Fall 2010.

¹⁷² Commission Communication to the European Parliament, The Council, The Economic and Social Committee and The Committee of Regions, A Digital Single Market Strategy for Europe, Brussels, 6.5.2015 COM(2015) 192 final, http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_en.pdf

4 Application to REVEAL

The following section applies the analysed legal regime to REVEAL. The application leads to legal recommendations that should guide the REVEAL Consortium in future actions. The application and the following recommendations should be read together with the previous chapters.

The previous chapters showed that the legal situation of internet intermediaries is far from clear. This is a relevant conclusion for REVEAL. Since REVEAL will be dealing with UGC we need to ensure that the REVEAL provider does not become liable for infringing content created by the third parties.

4.1 Role of REVEAL as an Intermediary

The OECD has defined the role of Internet intermediaries as *'bring[ing] together or facilitat[ing] transactions between third parties on the Internet. They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties.'*¹⁷³

The definition includes, for example, services such as Internet service providers (ISPs), hosting providers, search engines, e-commerce intermediaries, Internet payment systems and participative Web platforms. The definition has a broad scope, which makes it difficult for any online service not be covered by it. The REVEAL project is developing a platform intermediating and facilitating services between different actors: end users in journalism and enterprise, social media and social media users. REVEAL will also constitute a web platform involving UGC. We, therefore, qualify the REVEAL platform as an intermediary.

The E-Commerce Directive operates, with different definitions. Information Society service consists of *any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*. While the REVEAL platform will be undoubtedly provided at a distance, by electronic means and at the individual request of our end users, some might question the remuneration requirement. We should keep in mind, however, that the remuneration element of the definition is interpreted broadly. As explained above, it is sufficient if we can detect the existence of an economic activity or an activity for which an economic consideration is given in return. According to the exploitation plans for REVEAL the platform should continue its existence after the end of the project lifetime, as a commercial product. For that reason we consider the remuneration condition to be fulfilled.

The E-Commerce Directive foresees three liability exemptions for providers of intermediary services: mere conduit, caching and hosting. As we explained above, mere conduit and caching regimes, due to their technical specificity, do not apply to REVEAL. Qualification of REVEAL as a hosting regime is a more complex question.

Hosting service, according to the Directive, consists of the storage of information provided by a recipient of the service at his request. Typically, it concerns webhosting services that provide web space to their users, where users can upload content to be published on a website (e.g. YouTube).

REVEAL platform, strictly speaking, is not a classic hosting service, even though it will, most likely, store information. We could argue that the storage will occur on the request of the recipients of the service. This is because specific content will be indexed and stored by REVEAL only after a request

¹⁷³ OECD, The Economic and Social Role of Internet Intermediaries, April 2010, p. 9.

by an end user, placed through a search query. But the stored information will not be provided by the recipient of the REVEAL service, which is a condition for the qualification as ‘hosting service’ in the sense of Article 14 of the E-Commerce Directive. The stored information, in case of REVEAL, comes from third parties and is obtained from publicly available social media.

Despite the inapplicability of any of the liability exemptions offered by the E-Commerce Directive, we should not consider the conducted analysis a futile exercise. As an information society service, and an intermediary, REVEAL platform should act responsibly. This means that a standard requirement of reasonable duty of care still applies. This obligation refers to the processing of personal data by REVEAL, which was discussed in the previous deliverable. It also applies to the activities involving content created by third parties. Having in mind REVEAL’s role in facilitating access to content created by others, the platform should respect removal requests by entities whose rights might have been infringed (e.g. through defamatory statements or copyright violations). In essence, the responsible approach requires the platform provider to react to notifications about infringing content. It also requires REVEAL to respect ‘robot.txt’ (or codes such as ‘noindex’ or ‘noarchive’) and update its database and react to any changes applied to content at the original source (communicated via API, e.g. tweets removed from Twitter should not continue to be accessible via REVEAL). Before notification is issued, no knowledge of the infringing content can be attributed to the platform provider.

To support this line of reasoning, we refer to the CJEU case *L’Oréal v. eBay* where the Court applied the ‘storage but no knowledge’ approach.¹⁷⁴ The ‘storage but no knowledge’ approach provides a certain amount of flexibility in applying the existing legislation. It should also be supported because it allows integrating the new technical evolutions that have taken place since the adoption of the E-Commerce Directive in 2000.¹⁷⁵ Only in cases where the involvement of the service provider is such that knowledge or control may be inferred shall the provider lose the benefit of the liability exemption.¹⁷⁶ This line of thought can be detected also in the recent *Google Spain* ruling, where the Court clarified that search engines’ obligation to react to the removal request starts with the notification of an individual.

Effectively, such approach results in applying a solution similar to the one implied in art. 14 of the E-Commerce Directive (notice-and-take down). The conducted analysis, therefore, is useful because we are able to draw conclusions on how such removal mechanism should be applied in practice. The lessons learned, together with the articulated criticism, allow REVEAL to create a response mechanism that will be used to tackle any potential conflicts between the rights at stake. Apart from respect for the affected parties’ requests, the taken approach also minimises the risk of the platform’s liability for the infringing content created by third parties.

174 CJEU, Case C324/09, 12 July 2011.

175 P. Van Eecke, “Online Service Providers and Liability: a Plea for a Balanced Approach”, I.c., p. 1474.

176 C. de Callatay, “Les responsabilités liées aux messages postés sur internet: l’extension du régime d’exonération de responsabilité des intermédiaires aux acteurs du web 2.0”, I.c., p. 170. See also Court of Justice of the European Union, *L’Oréal v. eBay*, case C324/09, paragraph 123.

4.2 Legal recommendations for REVEAL platform (how to comply with the current regime)

To ensure that REVEAL does not become liable for third party content, a prompt reaction is required upon obtaining knowledge (e.g. through a notification) of the unlawful nature of the stored content. The notification needs to lead to assessment of the content in question and a decision to either remove or disable access to this content (or leave it intact if content is not illegal). At the same time, article 15 ECD should be emphasised, which states that a platform provider like REVEAL has no general obligation to monitor the information which he transmits or stores, nor to actively seek facts or circumstances indicating illegal activity. The general duties of care will arguably be satisfied when the REVEAL platform provider acts in accordance with these conditions.

To comply with the E-Commerce Directive conditions it is recommended that REVEAL takes the following steps:

- REVEAL platform should have a detailed Privacy Policy and Terms and Conditions for all the interested parties to obtain more information;
- REVEAL should also provide a contact point to provide more information;
- REVEAL should provide a webform where individuals could easily exercise their right to object and opt out from Reveal;
- A webform should also be provided to allow individuals requests to remove content infringing their rights (e.g. defamatory statements about them or content infringing their copyrights) to prevent REVEAL 's liability as intermediary for UGC;
- REVEAL should update the stored content to make sure that infringing content removed from the original sources (e.g. Social Media) does not continue to exist in the REVEAL platform;
- When a request for removal is filed an assessment of content must take place, in order to prevent censorship through a removal of legitimate (but critical) content;
- The removal request form should include the following information:
 - Name of the requesting party
 - Contact info (email) for further communication
 - Reason
 - Objection to data processing
 - Removal of illegal content
 - Field for a link to point out the specific location of the content
 - Field for explanation – although this is not obligatory to provide any justification it allows to better assess the request. Additional context about the request or the circumstances of the request will ensure that the decision made by REVEAL will not unduly curtail freedom of speech (or other rights).

5 Conclusions

The presented deliverable is the second one in the series of legal deliverables in REVEAL. Deliverable D1.2a explains the regime of intermediary liability in the European Union, as described in the E-Commerce Directive. It further focuses on relevant case law of the Court of Justice of the European Union and the European Court of Human Rights, and discussed the review process of the Directive by the European Commission.

The legal issues presented above have been taken into account by the REVEAL project. Legal compliance of the platform with the regime on liability of intermediaries is indispensable to fulfil the objectives of the project. Moreover, the exploitation potential of REVEAL will greatly increase due to this compliance. REVEAL assumes the position of hosting service provider. This means that REVEAL must react promptly upon obtaining knowledge (e.g. through a notification) about the unlawful nature of the stored content to remove or disable access to this content. Acting in this manner would arguably satisfy the general duties of care expected of a platform provider such as REVEAL.

REVEAL will closely follow the further developments of the *Delfi* case before the Grand Chamber of the ECtHR during the project lifetime. We will also keep following the review of the E-Commerce Directive and the newly announced strategy for the European Digital Single Market, with regard to platform responsibilities in combating illegal online content. Other areas of law, relevant for REVEAL, like compliance with the Terms and Conditions of the underlying social networks and media law will also be addressed at the later stage of the project.

6 References

Legislation

- [1] Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, 1950, http://www.echr.coe.int/Documents/Convention_ENG.pdf
- [2] European Union, Charter of Fundamental Rights, 2000, http://www.europarl.europa.eu/charter/pdf/text_en.pdf
- [3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive), O.J. L 281, 23 November 1995, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>
- [4] Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations, O.J. L 217/18-26, http://ec.europa.eu/enterprise/policies/single-market-goods/files/directive98-34/index_en.pdf
- [5] Directive 2000/31/EC of the European Parliament and the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce), O.J. L 178/1-16, 17 July 2000, <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=EN>
- [6] Greek Presidential Decree No. 131/2003 Implementation of Directive 2000/31 of the European Parliament and of the Council on certain aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce), Government Gazette (FEK) A 116, 16 May 2003
- [7] Council of Europe (Committee of Ministers), Declaration on freedom of communications on the Internet, 28 May 2003, <https://wcd.coe.int/ViewDoc.jsp?id=37031>
- [8] Council of Europe (Committee of Ministers), Recommendation CM/Rec(2012) 3 on the protection of human rights with regard to search engines, 4 April 2012, <https://wcd.coe.int/ViewDoc.jsp?id=1929429>
- [9] European Union, First Report on the Application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, at 13, COM (03) 0702, 21 November 2003, http://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2003/0702/COM_COM%282003%290702_EN.pdf
- [10] European Union, 'Online Services, Including e-commerce in Single Market', Commission Staff Working Paper, SEC(2011) 1641 final, http://ec.europa.eu/internal_market/e-commerce/docs/communication2012/SEC2011_1641_en.pdf.
- [11] European Union, Commission Communication to the European Parliament, The Council, The Economic and Social Committee and The Committee of Regions, A coherent framework for building trust in the Digital Single Market for e-commerce and online services, SEC(2011) 1640 final, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0942:FIN:EN:PDF>
- [12] OECD, The Economic and Social Role of Internet Intermediaries, April 2010, <http://www.oecd.org/internet/ieconomy/44949023.pdf>

[13] OECD, The Role of Internet Intermediaries In Advancing Public Policy Objectives, Forging partnerships for advancing public policy objectives for the Internet economy, Part II, 22 June 2011, <http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP%282010%2911/FINAL&docLanguage=En>

Case Law

[14] European Court of Human Rights nr. 64569/09 Delfi AS. v. Estonia, 10 October 2013

[15] European Court of Human Rights nr. 64569/09 Delfi AS. v. Estonia, 10 October 2013, [http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-126635#{"itemid":\["001-126635"\]}](http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-126635#{)

[16] European Court of Justice C-101/01, Lindqvist, 6 November 2003, <http://curia.europa.eu/juris/document/document.jsf?docid=48382&doclang=en>

[17] European Court of Justice C-236/08 to C-238/08, Google France and Google v. Louis Vuitton Malletier a.o., 23 March 2010, <http://curia.europa.eu/juris/document/document.jsf?text=&docid=83961&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=426784>

[18] European Court of Justice (Grand Chamber) C-324/09, L'Oréal SA and others, 12 July 2011, <http://curia.europa.eu/juris/document/document.jsf?text=&docid=107261&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=427023>

Opinions

[19] Opinion of Advocate General Jääskinen, Case C-131/12 Google Spain SL and Google Inc. vs. Agencia Española de Protección de Datos and Mario Costeja González, 25 June 2013, <http://curia.europa.eu/juris/document/document.jsf?text=&docid=138782&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=443725>

[20] Article 29 Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", WP 169, 16 February 2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

[21] Article 29 Working Party, Guidelines on the implementation of the Google Spain judgment, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20141126_wp29_press_release_ecj_de-listing.pdf

Publications

[22] R. J. Barceló and K. Koelman, Intermediary Liability In The E-Commerce Directive: So Far So Good, But It's Not Enough, *Computer Law & Security Report* 2000, vol. 4

[23] A.S.Y. Cheung, Liability of Internet host providers in defamation actions: From gatekeepers to identifiers, in Koltay, A. (Ed.), *Media Freedom and Regulation in the New Media World*, Budapest, Hungary: Wolters Kluwer, 2014

[24] IDATE, TNO, IViR, User-Created Content: Supporting a Participative Information Society, Study for the European Commission (DG INFSO), December 2008

[25] J. Iglezakis et al., Cyber Law, National Monographs, Greece, International Encyclopaedia of Law, available at: <http://www.kluwerlawonline.com/toc.php?area=Looseleafs&mode=bypub&level=6&values=Looseleafs~~IEL+Cyber+Law~National+Monographs~Greece>

- [26] H. Kaspersen and A. Lodder (eds.), *E-directive: guide to European Union law on e-Commerce: commentary on the directives on distance selling, electronics signatures, electronic commerce, copyright in the information society, and data protection*, Den Haag: Kluwer, 2002
- [27] J. Kokott and C. Sobotta, The Charter of Fundamental Rights of the European Union after Lisbon, *European University Institute, Academy of European Law*, 2010/6, <http://cadmus.eui.eu/handle/1814/15208>
- [28] A. Kuczerawy, SocloS deliverable D3.5, Legal and ethical analysis, 2012
- [29] A. Kuczerawy, Intermediary Liability & Freedom of expression: Recent developments in the EU Notice & Action Initiative, *Computer Law and Security Review* 2015, vol. 31, Issue 1
- [30] A. Kuczerawy and J. Ausloos, Case Study: European Union & Google Spain, NOC Report on Internet Intermediaries Liability, forthcoming
- [31] E. Lievens, *Protecting Children in the Digital Era e the Use of Alternative Regulatory Instruments*, Leiden: Martinus Nijhoff Publishers, International Studies in Human Rights, 2010
- [32] P. Valcke, M. Lenaerts and A. Kuczerawy, Who's Author, Editor and Publisher in User-Generated Content?, in Lambert P. (Ed.), *Social Networking: Law, Rights and Policy*, Dublin: Clarus Press, 2014
- [33] B. Van Alsenoy, A. Kuczerawy and J. Ausloos, Search engines after Google Spain: internet@liberty or privacy@peril?, *ICRI Working Paper Series*, issue 15/2013, 6 September 2013
- [34] B. Van Alsenoy, V. Verdoodt, A. Kuczerawy and G. Acar, Spion Deliverable D9.6.3, Evaluation of the legal framework applicable to Online Social Networks, January 2015
- [35] P. Van Eecke, Online Service Providers and Liability: a Plea for a Balanced Approach, *Common Market Law Review* 2011, vol. 48, issue 5
- [36] J. Van Hoboken, Legal Space for Innovative Ordering: on the need to update selection intermediary liability in the EU, *International Journal of Communications Law & Policy* 2009, Issue 13
- [37] T. Verbiest et al., Study on the liability of Internet Intermediaries, Markt/2006/09/E, 12 November 2007, http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf
- [38] J. Zittrain, A History of Online Gatekeeping, *Harvard journal of Law and Technology* 2006, vol. 19, issue 2